TUTTO QUELLO CHE GLI ALTRI NON OSANO DIRTI

2€ NO PUBBLICITÀ SOLO INFORMAZIONE E ARTICOLI

n.169

www.hackerjournal.it

HACKER JOURNAL

HARDWARE TEST

SCARICARE SENZA PC YES WE CAN!



HACKING

NEL CUORE DI UN MALWARE

EMULATORI

METTI IL SEGA SUL CELLULARE

PHISHING

DNS CACHE POISONING

HACKING

TUTTI I TRUCCHI DI facebook

QUATTORD. ANNO 9 - N° 169 - 5/18 FEBBRAIO 2009 - € 2,00

WLF PUBLISHING

hack·er (hăk'∂r)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

editoriale



Yes we can!

"Non chiederti che cosa può fare per te il tuo Paese, ma chiediti che cosa puoi fare tu per il tuo Paese.".
J.F.K.

Non si può scappare dalla pressione mediatica relativa al nuovo presidente degli Stati Uniti. Obama di qua, Obama di là, non c'è giorno che qualcuno non si inventi l'intervista al padre dell'amico del fratello del parrucchiere di Obama e via dicendo. Il momento è difficile e le aspettative - giustamente - sono alte. Tante e delicate sono le decisioni che aspettano il nuovo presidente in tutti campi.

Mi piacerebbe fare un piccolo elenco dei grandi problemi che affliggeranno il mondo nei prossimi anni e annoiarti con il mio punto di vista personale, ma non è questo il tempo né il luogo giusto per farlo.

Posso però fare un breve punto della situazione per ciò che riguarda il mondo della comunicazione e dell'Information Technology più in generale, mondi che il nuovo presidente ha dimostrato di conoscere decisamente meglio dei suoi predecessori.

- *Uno dei temi più spinosi riguarda sicuramente il diritto d'autore internazionale. Probabilmente l'argomento darà vita ad un nuovo filone di film post-western in cui i buoni sono le major e i cattivi gli utenti che condividono, con sfide all'ultimo sangue (degli utenti). Bisogna comunque creare una regolamentazione che cerchi di adeguarsi ai nuovi strumenti di fruizione dei contenuti.*

- *Altro argomenti spinoso riguarda la libertà d'espressione su Internet. Può sembrare un discorso semplice, ma cosa fare quando il Web diventa strumento di comunicazione per attentatori? O per mitomani che minacciano di fare stragi nelle scuole? O meno semplicemente per chi vuole fare sentire il proprio pensiero anche quando differisce da quello "di stato" (vedi i dissidenti Tibetani ad esempio)? CHI deciderà ciò che si può scrivere e leggere e con quale diritto?*

- *Chi controllerà che i provider vendano velocità davvero raggiungibili?*

- *Che le amministrazioni non controllino illegalmente l'email posta e i social network?*

- *Che le multinazionali non mettano spyware nei notebook per verificare le abitudini di marketing degli utenti?*

- *Che non sia sempre l'utente finale a pagare per furti di dati?*

- *Che non salti fuori qualche legislatore folle o semplicemente incompetente che in nome della sicurezza mondial-globale vuole controllare tutti bit che passano sulla Rete. Ovvero: Chi controlla i controllori?*

Beh, confesso che in questo momento non sono sicuro che vorrei essere al suo posto...

Buon lavoro signor Presidente.

Il Coccia

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 9 – N.169
5/18 febbraio 2009

Editore (sede legale):
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Realizzazione editoriale
a cura di BMS Srl

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Un malware truccato da Obama

Pochi giorni fa è stato scoperto un nuovo malware libero per il Web, che sfrutta la corrente in voga in questo momento di truccarsi da sito di divulgazione riportante notizie false ma plausibili. In questo caso, il sito riportava una presunta dichiarazione del neo-eletto Presidente degli Stati Uniti Barack Obama, nella quale lo stesso annunciava la propria rinuncia alla carica appena ottenuta. Facendo clic sul titolo di questa notizia, avveniva il download del malware vero e proprio, il cui nome avrebbe potuto ingannare i meno smaliziati (per esempio obamaspeech.exe). Una volta installato, il malware simulava in locale il funzionamento del sito delle news, mentre in background proseguiva con la propria natura di programma poco desiderabile, agendo liberamente sul computer dell'utente ignaro.



È importante notare fatto che chi immette in circolazione sistemi simili sfrutti le onde emozionali del momento, con notizie pertinenti e mirate in cui possono incappare persone poco esperte e quindi facili da ingannare. Non è la prima volta e non sarà nemmeno l'ultima, probabilmente. Un'altra importante annotazione risulta dallo studio del malware e della sua diffusione. I domini in cui si poteva incontrare erano diversi, e non solo riguardanti Barack Obama ma anche argomenti inerenti le appena trascorse festività natalizie e di inizio anno nuovo (siti di cartoline virtuali, per esempio). Ma la vera chicca è che tutti questi domini possono essere ricondotti a un solo provider cinese, Xinnet Technology Corporation. Naturalmente questo provider è stato immediatamente contattato dalle autorità internazionali per richiedere la rimozione di tutti i domini maligni, cosa che purtroppo non è stata ancora portata a termine, ma a quanto si sa non è la prima volta che Xinnet si rende complice (a questo punto non si sa fino a che punto involontariamente) del tentativo dei cracker, molto probabilmente cinesi, di creare una nuova botnet e si sa per certo che in passato ha ospitato l'opera noiosa degli spammer suoi connazionali e in certi casi operanti dalla Russia.

Non si capisce bene nemmeno il perché in Cina, Paese notoriamente poco permeabile al Net e alla libera circolazione delle informazioni sulla Rete, sia impossibile accedere a determinati siti di informazione occidentali, si venga controllati mentre si comunica con Skype e si viene fotografati quando si entra in un Net Cafè, ma nessuna autorità faccia niente quando malintenzionati abusano delle tecnologie a scopi maligni. Quando la censura va a corrente alternata.

CHROME VERSO LA 2.0

È passato poco più di un mese dall'uscita "ufficiale" di Chrome, il browser creato dai geni di Google, ma alcune voci parlano già di una versione 2.0 che verrà rilasciata a breve. Il nuovo Chrome dovrebbe integrare la possibilità di creare più profili di navigazione su un singolo Pc, in modo da adattare di volta in volta preferiti, cookie e cronologia in base a quale componente della famiglia sta utilizzando il computer in quel momento. Verrà migliorata l'integrazione con Windows Vista, consentendo a Chrome 2.0 di visualizzare correttamente le pagine scritte per Internet Explorer che il browser di Google non riesce ancora a "digerire". Se volete provare in anteprima la nuova versione del browser dovete registrarvi come sviluppatori al Google Developer Channel. Ricordatevi in ogni caso che Chrome è ancora in fase di sviluppo per cui potrà causare dei crash.



LA POLAROID DEL FUTURO

La macchina fotografica Polaroid è stata sicuramente un'icona degli Anni '80: la possibilità di scattare foto istantanee senza rullino e senza doversi rivolgere ad un fotografo per lo sviluppo, l'ha resa un vero must per i giovani di 20 anni fa. Con l'avvento delle fotocamere digitali il fascino di questa macchina sembrava svanito e invece Polaroid ha deciso di riprovarci lanciando la sua PoGo, una fotocamera a sviluppo istantaneo del nuovo millennio. La PoGo è completamente digitale, integra uno zoom ottico 4X, supporto per le schede SD e un pratico tool per il fotoritocco istantaneo: quello che però la rende unica è la microstampante integrata nella scocca, che permette di ottenere immediatamente stampe senza bordi da 5cm X7,5cm degli scatti più riusciti. La stampante utilizza una particolare carta denominata ZInk (Zero Ink) che garantisce foto dai colori brillanti e resistenti ad acqua, esposizione al sole e altre intemperie. Resta solo da capire se la nuova PoGo potrà replicare il successo di vendita della sua antenata.



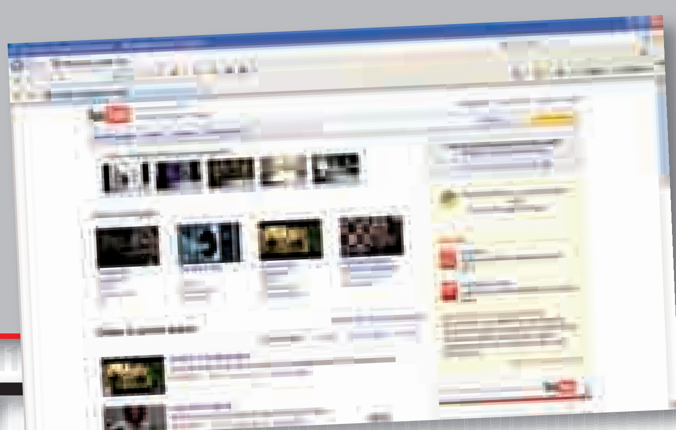
SILENZIO!

IL VIDEO È PROTETTO

Per fronteggiare la sempre più crescente diffusione di video protetti da copyright sul suo portale (con le conseguenti azioni legali), Youtube, il popolare sito di video sharing, ha messo a punto una particolare tecnologia in grado di riconoscere i filmati protetti e di eliminarne l'audio.

Al posto di dialoghi e musica apparirà una scritta in sovraimpressione che avvertirà i navigatori della mancata autorizzazione a riprodurre il filmato.

Infatti, nonostante le policy vietino agli utenti di Youtube di postare video protetti da copyright, i filmati che infrangono questa regola diventano ogni giorno più numerosi. Non potendo e cancellarli manualmente tutti, i responsabili del portale hanno pensato di adottare questo particolare software in grado di "mettere un bavaglio" ai video e alle proteste delle major cinematografiche.





IL GOVERNO INTERVIENE SULLA PIRATERIA

Tempi duri per i pirati italiani. Pochi giorni fa nella sala stampa di Palazzo Chigi è stato presentato il nuovo "Comitato tecnico contro la pirateria digitale e multimediale" un organismo che comprende tecnici, legislatori ed esperti delle forze dell'ordine incaricato di combattere il fenomeno della pirateria nel nostro Paese.



La novità introdotta da questo comitato riguarda i metodi con cui si intende debellare il fenomeno, affidandosi, più che a controlli serrati e leggi, alla sensibilizzazione degli utenti e l'autoregolamentazione di provider e portali web.

BLU-RAY DA VIAGGIO

Prima o poi doveva succedere. Dopo il boom dei lettori Dvd portatili adesso tocca ai nuovi dispositivi blu-ray il compito di intrattenere adulti e bambini durante i lunghi viaggi. Il primo produttore a sviluppare un lettore portatile blu-ray è stato Panasonic che pochi giorni fa ha presentato il DMP-B15 un dispositivo compatto dal design davvero particolare: dotato di un'apertura simile a quella di un notebook il coperchio del B15 è pensato per trasformarsi in un pratico supporto orientabile per migliorare la visione dei film. Ottima anche la durata della batteria che supera le 3 ore, mentre invece lascia perplessi lo schermo, da soli 8,9 pollici: con diagonali così limitate, si noterà davvero la differenza di qualità tra il lettore Panasonic e un qualsiasi altro Dvd da viaggio?



VIDEO CNN CONTAGIOSO

Il tempismo e l'ingegno di alcuni pirati informatici a volte è davvero eccezionale. Nei giorni scorsi l'RSA, l'organismo che si occupa di intercettare e fermare i virus che circolano sulla rete, ha scoperto un malware nascosto in un finto video sulla guerra tra Israele e lo Stato di Palestina della CNN. Lo strumento di diffusione è come al solito la mail: il messaggio, che ricalca perfettamente nella grafica e nello stile il format della CNN, invita gli utenti a collegarsi al loro portale per vedere il filmato ma, una volta avviato il player viene chiesta l'installazione di un plugin per visualizzarlo... ed ecco il virus: geniale!



Un codec tricolore per la supercompressione

Il codec più potente del mondo per la compressione di video e immagini parla italiano: a svilupparlo è stata l'azienda campana Eco Controllo, con il patrocinio del Ministero per lo Sviluppo Economico e la collaborazione di CNR, Università e Fondazioni. Dai test effettuati il nuovo codec riesce a comprime le immagini scattate dalle fotocamere, senza alcuna perdita di dati, del 51% in più rispetto all'ormai diffusissimo formato Raw e oltre l'84% in più dei file compressi in Tiff. Risultati eccellenti anche per i filmati: il codec infatti è riuscito a comprimere 3 filmati in formato standard PAL producendo file di dimensioni paragonabili a quelli compressi con i codec più diffusi (Mpeg 2 e 4, H264) ma con una qualità sensibilmente superiore. Ora occorrerà vedere quanto tempo ci vorrà prima che il nuovo formato passi i controlli di rito e diventi di pubblico dominio.



DANNI ALLE MAJOR

Ha fatto scalpore tra le principali major ed etichette discografiche, la sentenza di un giudice degli Stati Uniti che ha ritenuto inammissibile che la perdita in denaro di un file multimediale (film o canzone che sia) scaricato sia equiparabile ad un mancato acquisto. Le persone che scaricano selvaggiamente musica e video da Internet, questa è la tesi, non sarebbero mai disposti a spendere l'equivalente in denaro per arricchire la loro libreria multimediale, ma si limiterebbero a scegliere le cose che davvero gli interessano. Questa sentenza tuttavia ha aperto una breccia pericolosa per le industre musicali e cinematografiche che adesso troveranno molte difficoltà a dimostrare i danni economici reali subiti dall'azienda a causa della pirateria.



LE TV AL PLASMA COME I SUV

Le Tv al plasma inquinano quanto un SUV: è questo il risultato di un'indagine condotta da una ricerca inglese pubblicata dal quotidiano Indipendent.

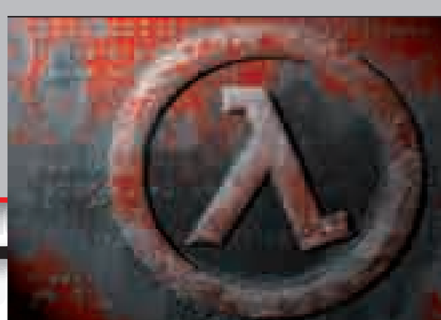


La ricerca ha messo in evidenza come le emissioni di CO_2 prodotte da un televisore al plasma da 50 pollici siano ben quattro volte superiori a quella di un TV di pari dimensioni con tecnologia LCD. Rispetto alle televisioni tradizionali questo valore sale addirittura di 50 volte. La notizia ha suscitato molte polemiche in Gran Bretagna, dove il governo di Gordon Brown si fa da sempre promotore di iniziative volte a ridurre le emissioni inquinanti, basti pensare alla nuova ZTL al centro di Londra o alla riduzione dei voli nell'aeroporto internazionale di Heatrow. Metterà una ZTL anche per i televisori?



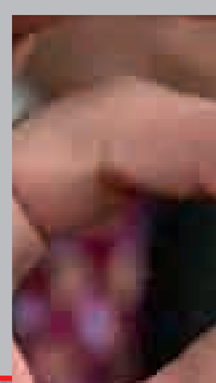
COLPA DEI DISTRIBUTORI

Scaricare un gioco senza pagarlo o comprarlo sulle bancarelle è un reato, questo lo sanno tutti. Tuttavia secondo Valve, famosa software house che ha sfornato titoli come Half Life e CounterStrike, la colpa non è proprio tutta degli utenti. È parere di Jason Holtman, responsabile affari legali di Valve, che spesso la lentezza nella distribuzione dei titoli di successo più recenti in alcuni Paesi, spinge chi vuole godersi l'ultima meraviglia 3D a cercare un "mercato parallelo" per procurarsela. Secondo Holtman, la soluzione sarebbe un lancio planetario di tutti i titoli più attesi che spingerebbe gli utenti a considerare l'acquisto. In effetti è triste sapere dell'uscita di un gioco e non trovarlo per mesi nel negozio sotto casa...



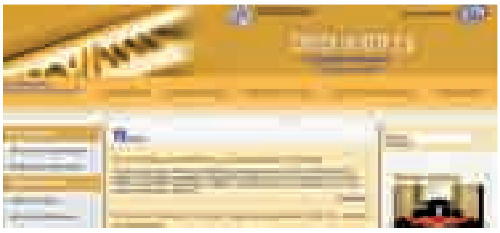
IL MISTERO IPHONE NANO

Ne parlano da mesi, ma ancora nulla è trapelato da Apple. Parliamo dell'uscita del famigerato iPhone Nano, una versione light dello smartphone più venduto nel mondo. Alcuni apple-maniaci infatti, sbirciando sui portali di custodie per



CHIESA 2.0

Le applicazioni Web 2.0 ormai sono diventate lo standard per la comunicazione online e il social networking. Non è quindi insolito partecipare o venire a conoscenza di forum su questa o quella nuova tendenza del Web.



Tuttavia fa sensazione che anche la Chiesa Cattolica si sia spinta a considerare il Web 2.0 come uno dei mezzi per veicolare il suo messaggio pastorale. La conferenza "Chiesa in rete 2.0" organizzata dalla CEI (Conferenza Episcopale Italiana) tenutasi la scorsa settimana, è stato un ottimo punto di partenza per sacerdoti, laici ed esperti di teconologie per confrontarsi su come e in che modo si possa parlare alle nuove generazioni utilizzando strumenti come MySpace, Badoo, Youtube o Facebook. In attesa di vedere quanto il Vaticano sia intenzionato a puntare sulle nuove tecnologie, anche se nella stessa conferenza è stato detto che FB estranea dalla vita reale, la Chiesa ha aperto un suo canale su Youtube... idea celestiale!

PIÙ 3D DI COSÌ

In questi giorni è uscito al cinema "Viaggio al centro della terra" remake dell'omonimo film degli anni '60 tratto dal romanzo di Jules Verne. Oltre all'uso smodato di effetti speciali, il "viaggio" di Verne potrà beneficiare anche del grande ritorno degli occhialini 3D colorati per un'esperienza stereoscopica che dovrebbe farci immergere ancora di più nell'azione del film.
Anche il produttore di chip video Nvidia sta lavorando ad un progetto simile per aumentare il coinvolgimento dei giocatori durante le loro partite.



Dopo aver migliorato l'animazione tridimensionale ai limiti della perfezione insomma, i futuri scenari del 3D puntano di nuovo sulle immagini stereoscopiche per fornire agli spettatori/giocatori un'esperienza ancora più "viva".

DOWNADUP CONFLICKER

Se questo nome non vi dice niente, allora cominciate a preoccuparvi. Downadup Conflicker è uno dei Worm più pericolosi che girano attualmente per la rete.
I suoi effetti sono devastanti sia per il sistema operativo (costringendo gli utenti alla re-installazione di Windows) sia per la rete che subisce blocchi e rallentamenti dovuti all'invio del virus. Downadup ha fatto strage su Internet contagiando in tutto il mondo ben 8,9 milioni di computer, 13 mila solo nel nostro Paese. F-Secure, che per prima ha rilevato la presenza di questo Worm, consiglia di installare (per chi ancora non l'ha fatto) un antivirus potente e un anti spyware e di aggiornare la protezione di Windows tramite l'Update del sistema operativo. Così potrete fare in modo che il nome Downladup Conflicker resti solo il ricordo di una vecchia minaccia informatica.

telefonini, hanno visto apparire nei listini prezzo, alcune cover per un misterioso iPhone Nano. Questo è bastato per scatenare i gossip sull'uscita di questo prodotto che dovrebbe andare incontro alle esigenze di coloro che trovano l'attuale iPhone troppo ingombrante per i loro gusti. Vedremo se a giugno (mese solitamente usato da Apple per i grandi annunci) si saprà qualcosa in più su questo prodotto.



LA REGINA DEGL SMS

Mandare messaggini SMS agli amici è da anni uno dei passatempi preferiti degli adolescenti, ma se pensate che il limite di 100 sms al giorno di alcune promozioni possa essere sufficiente per voi, questo non vale per la ragazzina americana che ha inviato in un solo mese ben 15428 messaggi.



Grazie ad una particolare tariffa promozionale dell'operatore AT&T il "conto telefonico" è stato di soli 30 dollari a fronte di un traffico generato di oltre 3000, altrimenti probabilmente la giovane tredicenne non avrebbe mai più visto un telefonino fino al compimento dei suoi 18 anni. Si tratta comunque di un fenomeno molto diffuso negli Stati Uniti dove le scuole non riescono a controllare l'utilizzo indiscriminato dei telefoni cellulari durante le lezioni.

Oggi sembra preistoria ma sono passati solo 40 anni dalla nascita del processore Intel 4004

DOVE TUTTO EBBE INIZIO





Una veduta del museo Intel e un'immagine pubblicitaria del chipset basato sul 4004.

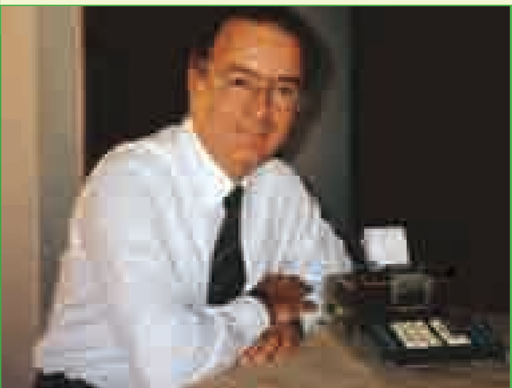
Senza questo piccolo frammento di silicio oggi non avremmo nè Internet, cellulari ed elettrodomestici e non avremmo nemmeno il computer e i suoi programmi. È nato da un'intuizione geniale e non sarebbe nemmeno dovuto esistere. Stiamo parlando del microprocessore Intel 4004, classe 1971, scopo principale l'implementazione di una calcolatrice su specifiche del committente, la Busicom.

:: La necessità

Busicom era un importante costruttore giapponese di calcolatori da tavolo degli anni Sessanta che aveva sviluppato un sistema modulare proprietario, in grado di sopperire alle diverse necessità di progetto. Per poter implementare nella pratica questo sistema, Busicom si rivolse a Intel, uno dei due maggiori produttori di chip dell'epoca (l'altro era Fairchild) in possesso delle tecnologie necessarie. In realtà, fino a quel momento Intel si era occupata prevalentemente di chip di memoria piuttosto che di microcontroller; tuttavia la sostanza tra gli uni e gli altri non cambia di molto e gli impianti usati per la produzione dei primi possono facilmente essere usati per produrre i secondi.
Al momento dello studio del progetto, Ted Hoff, uno dei responsabili di Intel, pensò che si poteva implementare il tutto con un solo chip generico basato su un sistema ROM+RAM anziché usare 12 chip dedicati, basati su ROM come proposto da Busicom. Dopo aver convinto sia il management di Intel sia il cliente Busicom della validità del progetto, nell'ottobre del 1969 venne firmato un contratto con cui Intel si impegnava a realizzare entro un anno il prototipo dei chip necessari. Fu una previsione troppo ottimistica, varie difficoltà incontrate durante lo sviluppo fermarono il progetto che così si arenò e giunse a un punto morto.

:: Il chip è italiano

Nell'aprile del 1970 Intel assunse Federico Faggin, proveniente dalla Fairchild, dove aveva inventato nuove tecnologie per la costruzione di transistor il cui terminale Gate è basato sul silicio anziché sull'alluminio come era prassi ai tempi. All'età di soli 19 anni, Faggin aveva collaborato alla costruzione dei primi computer Olivetti in Italia, prima di trasferirsi negli USA per terminare gli studi.



Federico Faggin con il prototipo funzionante del calcolatore Busicom basato sul suo microprocessore.

Dal momento del suo ingresso nel team di sviluppo del 4004, Faggin assunse di fatto la posizione di leader di progetto e sfruttò la tecnologia al silicio da lui inventata per l'implementazione del chip. Non solo: creò anche un nuovo modo di concepire il disegno del core, che fino ad allora era basato su forme standard dei componenti ripetute identiche a se stesse e che portavano inevitabilmente a chip molto più grandi. Con la riprogettazione della forma dei componenti in maniera adattiva, Faggin riusciva a ricalcare quasi perfettamente lo schema del progetto teorico di un chip sul supporto del core, ottimizzando gli spazi e producendo quindi chip meno ingombranti e meno avidi di potenza (Random Logic Design). Con notevole ritardo sulla data di contratto, il primo microprocessore Intel della storia vide comunque la luce e fu usato dal committente esclusivo Busicom nei propri prodotti. Il chipset comprendeva il 4001, una ROM da 2048 bit con porta I/O programmabile a 4 bit; il 4002, una RAM da 20 locazioni da 4 bit con 4 registri e porta di uscita a 4 bit; il 4003, un chip di espansione con ingresso seriale e uscita seriale/parallela; e infine il microprocessore 4004, contenente 2300 transistor distribuiti su un'area di circa 7x9 millimetri. Questo microprocessore poteva eseguire oltre 60.000 operazioni al secondo e aveva maggior potenza di calcolo del primo computer mai costruito, l'ENIAC, che era grande come l'intero piano di una palazzina e conteneva oltre 18.000 valvole. Con questo chipset, Busicom produsse e vendette oltre 100.000 calcolatori a clienti in tutto il mondo. Ogni core dell'Intel 4004 riporta in un angolo le iniziali F.F. come firma di Federico Faggin, senza il quale il processore non avrebbe mai visto la luce.



Il calcolatore Busicom con chipset Intel. Notizie sul 4004 si trovano sul sito www.4004.com e su www.intel4004.com.

:: Non tutto rose e fiori

Purtroppo, come succede spesso nel caso di importanti scoperte o invenzioni, la paternità delle stesse è spesso contesa tra più soggetti. Nei casi migliori si riesce a raggiungere degli accordi, nei casi peggiori si finisce inevitabilmente in tribunale per lunghe ed estenuanti battaglie legali che spesso non vedono mai la fine.
Fino a non molto tempo fa, Intel e i suoi responsabili hanno sempre minimizzato l'importanza della partecipazione di Faggin al progetto, tanto da assegnarne ufficialmente la paternità al solo Ted Hoff. Non solo: per rincarare la dose, la tecnologia al silicio apportato da Faggin ai laboratori Intel finì sotto brevetto da parte di Hoff come propria invenzione. Solo dopo molte pressioni da parte dello stesso Faggin Intel acconsentì a dare il giusto peso al nome del nostro compatriota, ma tuttora non vuole ammettere che il vero leader di progetto che portò alla nascita del primo microprocessore della storia fu proprio Faggin. Tra l'altro, per sottolineare invece quanto fondamentale sia stato il suo contributo per Intel, a lui vanno attribuiti anche il merito di aver reso commercialmente disponibile senza esclusive il microprocessore Intel, l'ideazione di nuovi modi per usare le nuove tecnologie da lui inventate (pensiamo per esempio ai sensori CCD che popolano le nostre fotocamere digitali) e la nascita in seguito dei primi microprocessori Intel a 8 bit, l'8008 e l'8080, quest'ultimo antesignano dell'8088 e dei moderni processori multicore.

:: Rest In Peace

Oggi il glorioso 4004 non viene più usato, naturalmente, superato e migliorato dalle nuove tecnologie e inadatto per soddisfare le moderne esigenze di mercato. Riposa in pace in un museo appositamente creato da Intel per celebrarne il 35° compleanno nel 2006, nella sede centrale dell'azienda. Nel 2007 è stata organizzata una reunion del team di sviluppo del 4004, a cui tutti noi, appassionati di elettronica e di informatica, vogliamo solo dire grazie in eterno.



Il team di sviluppo del 4004 nel 2007: da sinistra, Ted Hoff, Hal Feeney, Stan Mazor, Masatoshi Shima (Busicom) e il nostro Federico Faggin.



Scopriamo come funziona una delle tecniche di attacco più semplice e pericolose

DNS AVVELENATI

È un tipo di attacco già noto da più di dieci anni: il pericolo viene dal fatto che i server DNS che, per comunicare tra loro, usano riferimenti (Query ID) abbastanza facili da prevedere. Questo attacco richiede meno conoscenze di quello che si potrebbe pensare e viene anche facilitato dal fatto che il programma BIND sia facilmente prelevabile da Internet. Bastano così un po' di pratica e di studio del programma per rendersi conto che quello che dovrebbe essere il cuore della comunicazione dei server DNS ha qualche problema.

:: Come funziona

Prima di tutto, che cosa fanno i server DNS tutto il giorno? Semplice, trasformano i nomi come www.google.it in un indirizzo IP (es. 123.12.134.123) comprensibile per le macchine e che contiene tutte le informazioni per raggiungere il server desiderato. Ma se l'abbinamento tra un sito e il suo vero IP viene modificato, la comunicazione viene di conseguenza dirottata a un diverso indirizzo IP. Potrebbe sembrare solo uno stupido scherzo, ma se pensiamo per esempio ai servizi bancari online, è evidente che la cosa potrebbe essere assolutamente nefasta: ci colleghiamo, diamo utente e password al sito fasullo che impersona quello della nostra banca e intanto qualcuno accede alla banca usando i nostri dati e i nostri soldi. Non è carino!

:: Il DNS canonico

Durante una comunicazione sul Web, prima che le informazioni appaiano nel nostro browser vengono compiuti diversi passaggi, di cui normalmente non abbiamo notifica. Se per esempio cerchiamo www.google.it, il browser inoltra la nostra richiesta, che viene trasmessa fino al primo DNS disponibile e configurato in **Schema 1**. L'informazione su quanto tempo considerare valido il sito della nostra ultima richiesta DNS viene espressamente fornita del Server B (ammesso che B abbia trovato nel suo elenco tale informazione) e viene denominata TTL (Time to Live). Alla scadenza, la richiesta deve essere verificata di nuovo.

:: L'anello debole

La Query ID, o QID, serve per tenere ordinate e separate le varie interrogazioni fatte al server. È un po' come il numerino che prendiamo al supermercato per fare la fila, ogni cliente ha il proprio e il negoziante serve i clienti uno alla volta seguendo l'ordine dei numerini.



In una normale richiesta DNS, il resolver (Bob) vuole sapere come raggiungere il server di Anna e lo chiede server DNS, che risponde con l'IP corrispondente al server corretto.



In un attacco DNS cache poisoning, Eva invia false risposte al server fino a quando la QID non è corretta e quindi la cache del server ISP viene modificata fino alla scadenza della TTL con l'IP maligno.

Per convenzione i primi 16 bit dei pacchetti TCP sono utilizzati per inserire questo identificatore univoco. Questo sistema però presenta una marcata vulnerabilità. Poniamo il caso che Bob sia il resolver e Anna un server DNS. Nascosta nell'ombre c'è Eva. Bob si collega ad Anna e le chiede l'indirizzo www.vittima.com. Anna trova nel suo elenco che 1.2.3.4 = www.vittima.com, ma Eva vuole che la risposta sia 6.6.6.0. Siccome Eva non può vedere la QID dei pacchetti di Bob, la sua QID non coinciderà con quella di Bob. Questa è la difesa che ha Bob per la sua navigazione, ma di solito l'attacco QID, è iniziato tempo prima e il server continua a ricevere le richieste di Eva.
Nel frattempo BIND semplicemente incrementa la QID per ogni risposta, come il cartellino nel negozio. Quindi il DNS server crea le sue QID ad esempio 4001 e poi 4002: sarà facile indovinare che la prossima sarà 4003? Eva quindi cerca di inviare una risposta con il QID 4003; se ci riesce, Eva ha vinto.

:: Avvelenare la cache

Ovviamente se la generazione delle QID fosse assolutamente casuale e un po' più sicura il problema non sussisterebbe. Ma torniamo alla connessione. Anna vede che Bob gli ha mandato dei pacchetti di dati e conosce pure la corretta QID, mentre Eva deve provare a indovinarla o scoprirla.
Il primo dei due che riesce a inviare il pacchetto con la giusta QID vince. Le probabilità per Eva sono comunque scarse e se perde questa partita non potrà riprovarci per molto tempo, perché le informazioni sulla cache sono state validate fino alla TTL. Ma potrebbe provarci con un altro schema e avere maggiori possibilità di successo.

I nomi www.vittima.com, clienti.vittima.com o mio.vittima.com sono riferiti alla stessa macchina, quindi i record nella cache del DNS server sono equivalenti. Ma questo provoca anche un errore di logica: creando una serie di false query per 1001.vittima.com, 1002.vittima.com e così via, Eva potrebbe alla fine indovinare la QID arrivata al nome 1099.vittima.com, e quindi modificare il file di cache del server DNS. Il server salverà le informazioni aggiuntive per il dominio 1099.vittima.com in una particolare sezione del file di cache che si chiama ADDITIONAL SECTION. Terminato l'aggiornamento, tutte le future richiesta per vittima.com effettuate su quel server, non solo da Bob ma da tutti gli utenti che volessero visitarlo, verranno dirottate all'IP 6.6.6.0 come desiderato da Eva.

:: Conclusioni

Si sono verificati casi famosi in cui digitando l'indirizzo di un server si veniva dirottati da un'altra parte. Oggi le difese sono state migliorate e i server DNS patchati per evitare attacchi di questo tipo (quasi tutti, per lo meno). Anche BIND è stato migliorato nelle ultime versioni. Tuttavia l'aggiornamento effettivo dei server va a rilento e potrebbero volerci anni prima che si possano evitare completamente attacchi di DNS cache poisoning.

[Schema 1]

1) noi scriviamo www.google.it sul browser;
2) il browser chiede al sistema di gestione di rete di essere messo in contatto con il sito www.google.it;
3) il sistema cerca nel file hosts se trova una corrispondenza e non la trova;
4) contatta il server del provider;
5) l'ISP contatta il primo server DNS e invia la richiesta;
6) se il server DNS in questione, chiamiamolo A, non ha al suo interno l'informazione relativa a dove si trovi google.it allora inizializza una richiesta al suo server DNS più vicino;
7) il server che riceve la richiesta, chiamiamolo B, provvede prima di tutto a creare una Query ID, poi si mette a cercare il nome e se non lo trova interroga un altro server e così via;
8) se viene trovata la corrispondenza, il nostro browser, dopo che Server A avrà preso nota nella sua cache, verrà messo in contatto con il sito e finalmente potremo cercare quello che ci interessa.



L'alba di un nuovo Lego

Cambiamo il firmware dei Lego NXT e programmiamolo per costruire veri robot ai nostri ordini

Nel 2006, Lego ha presentato MindStorm NXT, un concentrato di tecnologie, pensato per sperimentare di persona la programmazione di robot anche complessi Il cuore del sistema è un grande mattone che contiene un processore ARM AT91SAM7S256 a 32 bit e che mette a disposizione una serie di risorse tra cui una porta USB, 4 porte di connessione per i sensori, 3 porte per collegare motori, un sistema di connessione bluetooth di classe II e un display LCD 100x64. A questo centro nevralgico si possono collegare 3 motori passo passo, un sensore di tocco, un sensore di luce, un microfono e un sensore di distanza basato sugli ultrasuoni, tutti inclusi nel kit E in caso di necessità, il kit può essere ulteriormente espanso con vari tipi di sensori). A completamento del kit NXT è fornito un software di programmazione visuale, sviluppato per rendere semplice la realizzazione di programmi anche ai digiuni di informatica. E qui sta il suo limite: come tutti gli ambienti completamente visuali, permette di sfruttare solo in minima parte tutte le sue potenzialità. Lego ha pensato anche a questo e ha al rilasciato il firmware originale con licenza Open Source, consentendo di sostituire il firmware dell'unità centrale con uno diverso, prodotto da terzi.



Il sistema di programmazione proposto da Lego per l'NXT è semplicissimo da usare ma permette di creare solo programmi piuttosto semplici.



leJOS è un'estensione del java Development Kit rilasciato gratuitamente da Sun. L'installazione di quest'ultimo è obbligatoria per poter programmare il nuovo firmware dell'NXT.



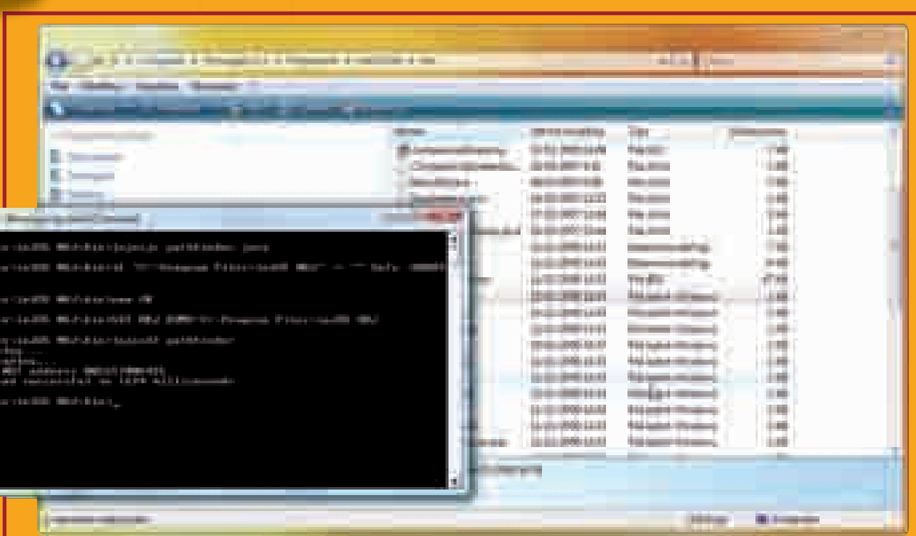


Sul sito di leJOS troviamo informazioni e notizie sul sistema NXT.

Uno dei più interessanti si chiama leJOS ed ha una caratteristica unica: trasforma il sistema NXT in una Java Virtual Machine, programmabile come qualsiasi altra VM simile. In più, trattandosi di una VM che funziona su un hardware particolare, leJOS dispone di estensioni speciali che, tramite semplici API, ci permettono di controllare e pilotare l'hardware a nostra disposizione. A completamento del nuovo firmware i creatori di leJOS ci mettono a disposizione anche un compilatore adatto al sistema NXT e alcuni programmi di utilità. Un altro vantaggio dell'uso di leJOS rispetto al firmware originale è che leJOS ha tempi di reazione decisamente più veloci.

:: Passare a leJOS

Il primo passo per sostituire il firmware è quello di scaricare dal sito lejos.sourceforge.net il programma di installazione di leJOS NXJ. Se ancora non l'abbiamo sul nostro computer dovremo anche scaricare dal sito java.sun.com un development kit di Java (JDK) e installarlo. Allo stesso modo dovremo avere installato sul computer il driver per il collegamento dell'unità NXT, scaricabile dal sito mindstorms.lego.com/support/updates.



La compilazione di un programma Java e l'invio successivo all'unità NXT si eseguono da riga di comando DOS e non richiedono che pochi secondi.

Colleghiamo l'unità NXT al computer tramite USB o Bluetooth, accendiamola e avviamo il programma di installazione di leJOS. Dopo l'installazione dei file di supporto, leJOS provvederà automaticamente all'aggiornamento del firmware. Una volta completata la procedura, l'unità NXT si riavvierà presentando il loogo leJOS in sostituzione di quello originale e il menu dell'unità sarà decisamente diverso: non saranno più presenti i programmi di esempio ma verranno mostrati dettagli tecnici come la memoria disponibile. Come ultimo passo prima di iniziare a usare leJOS dobbiamo assicurarci che sul nostro PC siano correttamente impostate le variabili d'ambiente LEJOS_HOME e JAVA_HOME, in modo che indichino, rispettivamente, i percorsi di installazione di leJOS e del SDK di Java. Se usiamo Windows Vista, inoltre, è richiesto un altro piccolo sforzo: dovremo modificare con un editor di testi i file lejosdl.bat e lejosjc.bat contenuti nella cartella BIN del programma, eliminando in entrambi i file la riga @if NOT %lejos_home:~-3% == nxj GoTo :DONE. A questo punto abbiamo a nostra disposizione tutto il necessario per iniziare a creare programmi Java funzionanti con il nostro NXT.

:: Il Lego prende vita

Per un riferimento completo alle API che leJOS ci mette a disposizione possiamo consultare il sito stesso da cui abbiamo scaricato leJOS. Nella documentazione sono compresi diversi esempi che mostrano anche tecniche per integrare le tecnologie a disposizione: creare robot comandati via Bluetooth dal PC o dal cellulare, sistemi di navigazione che usano anche sensori aggiuntivi e molte altre idee, a volte già pronte. Dopo aver realizzato il programma e un modello Lego NXT su cui installarlo, dovremo provvedere alla sua compilazione. Basta aprire un prompt dei comandi, andare nella cartella in cui abbiamo salvato il nostro codice java e avviare il compilatore leJOS con il comando lejosjc seguito dal nome del file interessato. Il secondo passo sarà quello di accendere l'NXT e collegarlo al computer via USB o tramite Bluetooh. Poi diamo il comando lejosdl seguito dal nome del programma da caricare sull'NXT, senza estensioni. L'NXT avvierà automaticamente il programma che abbiamo caricato.

Come i ricercatori hanno creato una botnet benigna (ma comunque illegale)

UNA BOTNET ANTI-BOTNET

Abbiamo tutti ben presente cosa sia una botnet: una grande rete di computer infetti e agli ordini del cracker che l'ha creata, che viene usata per portare attacchi verso siti o altri computer. Si tratta quindi di un'entità maligna, dalla sua creazione (che avviene di solito via virus o malware) al suo utilizzo, contro cui l'uniche armi oggi realmente disponibili sono l'informazione e la prevenzione.

:: Il sistema tradizionale

Quando si scopre di essere infetti da un malware, un trojan o comunque da un virus che trasforma il nostro PC in uno zombie entrato a far parte di una botnet maligna, l'unica maniera per uscirne è usare un antivirus adeguato. Ma non sempre funziona: i cracker sono sempre più scaltri e i sistemi che adottano per installare sui nostri computer il loro software sempre più difficili da debellare. Ciò che possiamo veramente fare è stare sempre all'erta: antivirus e antimalware, quindi, ma questo va bene per chi sa il pericolo che corre navigando sul Web.

La maggior parte degli utenti di Internet però ha solo le conoscenze di base del sistema e spesso si affida a ciò che trova preinstallato sul computer, senza premurarsi di tenerlo aggiornato o di mantenere adeguato il proprio livello di sicurezza. È quindi palese che la strategia più corretta da seguire è quella di diffondere le informazioni di base sulla sicurezza informatica, per impedire ai cracker di trovare persone con la guardia abbassata e, di conseguenza, minori rischi di trovarsi una serie di PC infettati e la possibilità di realizzare nuove botnet maligne.

:: Le armi del nemico

Nel 2007, Thorsten Holz ha presentato in occasione del congresso 24c3 un metodo per debellare una botnet comandata da Zelathin, che però coinvolgeva non meno di 65536 computer. Una cosa non molto fattibile, secondo gli studiosi tedeschi Georg Wicherski, Tillmann Werner, Felix Leder e Mark Schlösser. Questo li ha spinti a cercare una soluzione diversa, più fattibile e alla portata di chi dovesse mettersi a caccia di botnet per distruggerle. La loro soluzione ha del particolare, se così vogliamo dire: usa le stesse armi del nemico che vuole combattere, nascendo sotto forma di "malware benigno" e comportandosi, né più e né meno, come la stessa botnet che vuole smantellare. Il programma si chiama Stormfucker, nome abbastanza pittoresco, e la botnet che intende debellare è per l'appunto la rete Storm, basata su Zelathin.

:: Il punto debole

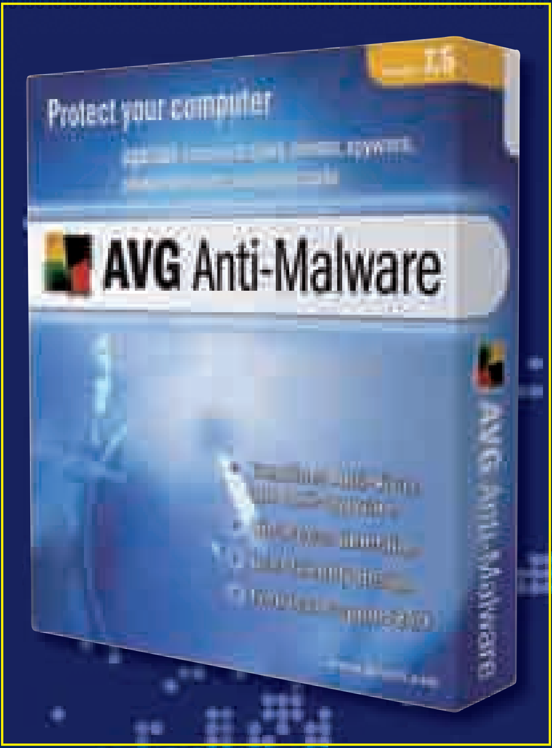
Studiando i binari di Zelathin, i ricercatori tedeschi hanno scoperto che in realtà per impartire un comando a una rete basata su questo sistema non occorre affatto essere autenticati, non occorre un vero e proprio login. Tutti i nodi che vengono aggiunti mediante NAT infatti compiono un semplice XOR a 4 bit per verificare che il comando ricevuto



giunga da una fonte “certificata”. Basta quindi implementare il protocollo server in maniera adeguata per prendere il controllo di questi nodi, anche non facendo parte del gruppo di cracker che ha creato la botnet. Unica eccezione i nodi che accedono senza traduzione degli indirizzi di rete (NAT): in questo caso infatti il malware si aspetta una chiave RSA a 64 bit, molto più difficile da craccare, pertanto questi nodi non possono essere controllati.

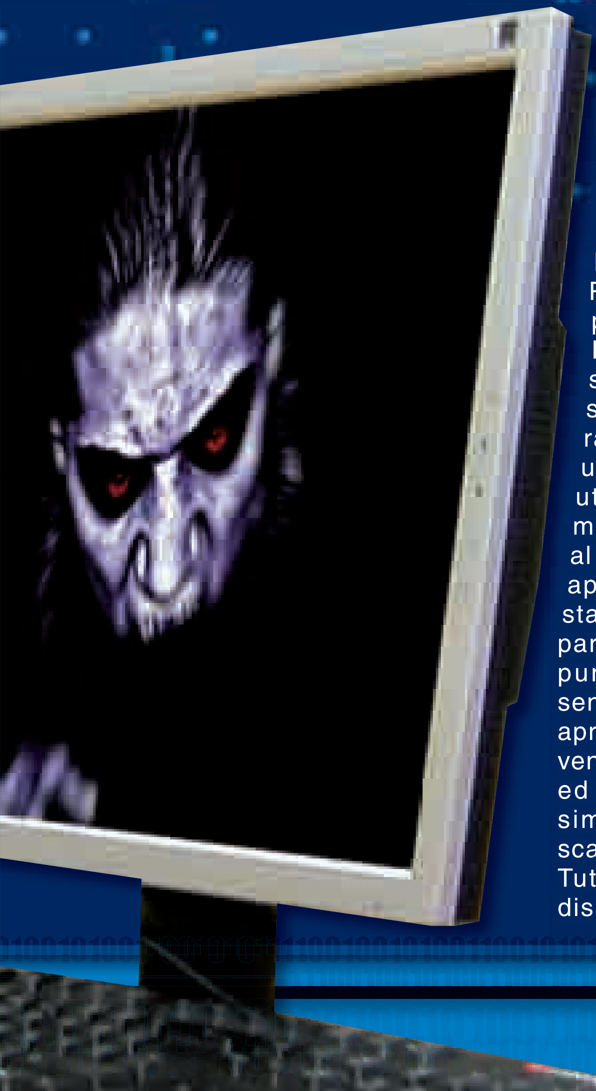
:: Attacco alla botnet

Stormfucker quindi si rivolge a quei nodi che risultano più facili da controllare, inviando loro un comando di autenticazione fasullo che però questi reputino valido. A questo punto avviene il vero e proprio attacco alla botnet: lo zombie che è stato raggiunto (e quindi per iniziare ne basta uno, non 65536 come nel metodo di Holz) in base a questo comando scarica quello che reputa un aggiornamento del malware da un server mantenuto dai “buoni”, che si occupa in realtà di disinfettare la macchina su cui è in esecuzione il software maligno. Allo stesso tempo, questo zombie invia il medesimo comando ad altri PC zombie della botnet, i quali si comporteranno nella stessa maniera, scaricando il software benigno e inviando a loro volta il comando di disinfezione ad altri PC. In poco tempo, quindi, buona parte degli zombie della botnet dovrebbero essere distaccati dalla stessa e contemporaneamente disinfettati, rendendola inutilizzabile o per lo meno rallentandone le operazioni.



Prevenire è sempre meglio che curare: installiamo un buon antivirus-antimalware per stare più tranquilli.

:: L’altra faccia della moneta



Il problema nell’implementazione di un sistema come quello appena descritto sta nel fatto che il tutto avviene all’insaputa dell’utente, proprio come in origine ha avuto luogo l’infezione. Purtroppo una tale pratica è completamente illegale in moltissimi Paesi, e quindi non attuabile, pur se i risultati ottenuti in fase di sperimentazione sono stati incoraggianti. Si potrebbe pensare a un servizio a richiesta, in cui un utente accetta termini che permettano a enti preposti di inviare al proprio PC comandi e software appositamente creati per disinfestarlo da malware che lo rendono parte di una botnet, ma su questo punto i ricercatori tedeschi dissentono: difficilmente chi scarica e apre allegati di posta di dubbia provenienza si rende conto del pericolo ed è a conoscenza di operazioni simili, non firmerebbero mai per scarsa conoscenza della questione. Tuttavia gli stessi ricercatori non disperano che un giorno, in realtà in cui le autorità vogliano veramente liberarsi da piaghe come le botnet maligne, possano agire promuovendo leggi apposite che permettano l’uso di simili tecnologie. In alcuni casi si tratta di modi di agire già adottati e sperimentati, anche se in forma molto ridotta, pertanto tutto è possibile, si tratta solo di volerlo.

:: E le nuove botnet?

Tutto il software si migliora: lo fanno i programmi normali, per così dire legittimi, e lo fanno anche i software maligni come i virus e i malware. Le nuove botnet non sono più così semplici da attaccare come quelle gestite da Zelathin, usano sistemi di crittografia molto più complessi e difficili da decrittare, sono insomma diventate più furbe.
Non sono comunque infallibili: grazie alle nuove tecnologie utilizzate richiedono più tempo per trovare le falle al loro interno ma sono comunque destinate ad essere sconfitte dall’utilizzo di soluzioni tecnologiche sempre più radicali.



Mettiamo a nudo il social network che sta facendo impazzire gli italiani

TUTTI GLI HACK DI FACEBOOK

A volte, basta una parola: Facebook. Ed ecco che si apre un mondo online. Un social network che, da solo, vale oltre 160 milioni di utenti.
E una somma di denaro che, stando alle ultime stime, supera i 16 miliardi di dollari. Notorietà, utenti, denaro... ci sono tutti gli ingredienti per una storia di successo di sola andata, ma c'è chi maligna che la struttura software di questo sistema non si sia evoluta di pari passo con la sua celebrità.
E così, ecco storie di "sviste" che sono costate la sicurezza di migliaia e miglia di profili, con relativi dati personali. In questo caso non serve chissà quale esotica tecnica hacker: basta un po' di social engineering. Si crea un falso profilo, magari di un personaggio famoso (meglio se non troppo) e si chiede di entrare a far parte del "circuito" di amicizie di un utente. Poi, si spende qualche settimana a osservarne abitudini e vicissitudini, grazie ai messaggi che pubblica e riceve. Il piatto è servito: si inizia a comunicare, con chiari riferimenti alla sua sfera privata, ottenendo tutte le informazioni che si desiderano.



Facebook fu creato nel 2004 dal diciannovenne Mark Zuckerberg, di cui attualmente è Amministratore Delegato.

::Una foto, molte foto

Ma l'hacking di Facebook non deve essere visto solo in un'accezione negativa. La struttura paleolitica del software che lo gestisce infatti, si presta a molte ottimizzazioni da attuare con grande semplicità.
Uno dei più sfiziosi è quello che consente di guardare un album di foto amnche se questo non è di utente che fa parte dle nostro network. Chi conosce Facebook, infatti sa che se un amico è "taggato" in un album di utente conosciuto, non è possibile vedere le altre

foto della raccolta. Lo script “Facebook View Photo in Album”; disponibile su http://userscripts.org/scripts/show/9580, ci consente invece di attivare il comando “See this photo in its album”. In questo modo, abbiamo accesso a tutte le foto di quell’album. Se un nostro amico, invece, ha scelto di limitare l’accesso ai propri album fotografici, arriva in nostro soccorso lo script “View All Photos” (http://userscripts.org/scripts/show/11218). È così potente da abbattere eventuali impostazioni di privacy relative alle foto, dandoci libero accesso agli album.
Non funziona in tutti i casi, ma vale di sicuro la pena provarlo.

::Dal generale allo specifico

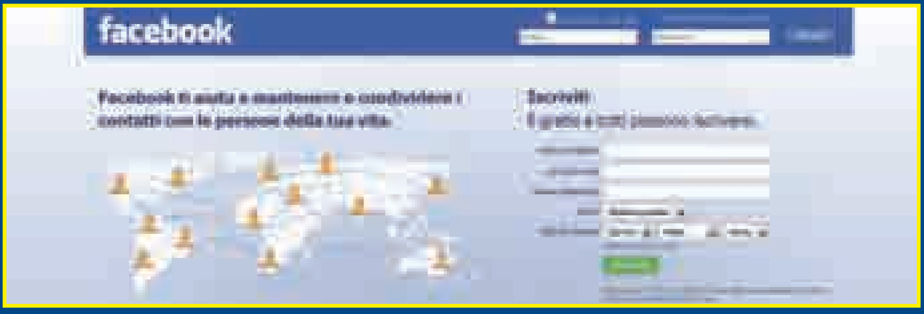
“FB People Redirect”, invece, è uno script che consente di visualizzare il profilo dettagliato di un utente del quale si conosce solo la pagina Facebook. Un po’ come accade con servizi come LinkedIn, infatti, un utente di Facebook ha due tipi di profilo: uno pubblico, che compare di solito anche su Google, e uno con maggiori informazioni, disponibile invece ai soli iscritti al network.
Lo script “FB People Redirect” (http://userscripts.org/scripts/show/27011) ci consente, appunto, di visualizzare anche I secondo. Il consiglio, però, è di attivare lo script solo una volta che ci siamo autenticati in Facebook, altrimenti c’è il rischio di scatenare un “loop” che porta al crash del browser.
Per un paio di hack dedicati a rovinare, un po’, la privacy, eccone uno che invece tutela la nostra. Si tratta di Private Wall (http://www.facebook.com/applications/Private_Wall/20221093560), ed è un’applicazione Facebook, sconosciuta a molti, che protegge il nostro “wall” privato dagli sguardi indiscreti. Solitamente, infatti, i messaggi che compaiono sul n ostro muro virtuale, in Facebook, sono alla mercé degli sguardi degi iscritti al nostro network. E questo non sempre è un bene, specie per questioni più “incognite”. “Private Wall”, invece, rende inaccessibili questo spazio, senza bisogno di cambiare le impostazioni sulla privacy del nostro account Facebook.



Uno degli hacking più noti di FB si basa sul social engineering: basta spacciarsi per qualcuno di famoso, ma “credibile”.

::Pubblicità? No, grazie!

Parlando di privacy, c’è da dire che anche i numerosi messaggi pubblicitari visualizzati su Facebook la minano. Per eliminarli, in un solo colpo, c’è uno script dal nome molto eloquente. Si tratta di Remove All Facebook Ads (http://userscripts.org/scripts/show/13787). La raccomandazione è di tenere spesso d’occhio il rilascio di nuove versioni, che aggirano le soluzioni trovate da Facebook, di volta in volta, per far comparire comunque la pubblicità. Se invece è proprio la pubblicità che cerchiamo, intesa come business, Facebook Advertising (http://www.facebook.com/advertising/) è l’applicazione che fa per noi. Si tratta, infatti, di un potentissimo editor di pubblicità per Facebook, che oltre a permetterne la rapida e completa creazione, consente di tenere traccia dei suoi fruitori.



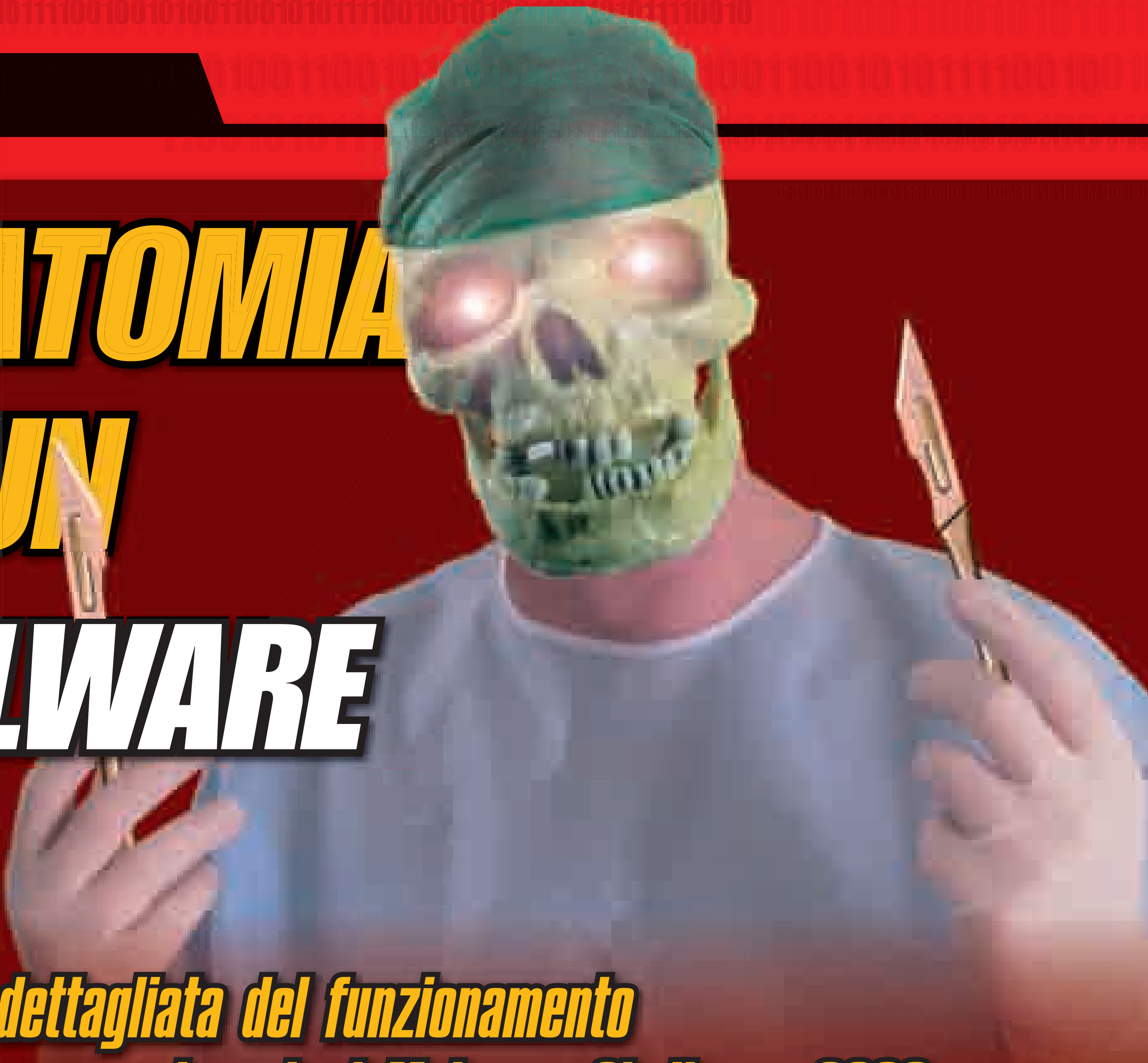
La maggior parte degli hack di Facebook richiedono l’autenticazione. Per questo, è bene crearsi prima un profilo, anche se fasullo, ed effettuare il login.

Facebook Refresh Alpha 2 Alpha (http://userscripts.org/scripts/show/24225) è uno script che, semplicemente, aggiorna Facebook ogni 30 secondi. Sembra una cosa da poco? Chi è solito utilizzare molto questo social network apprezzerà, invece, il valore aggiunto di uno script che raddoppia la sua “produttività”. Al momento, Refresh Alpha 2 si occupa di aggiornare il feed delle news, le notifiche e il numero di messaggi ricevuti; ma è in lavorazione una nuova versione che si occuperà di aggiornare anche i messaggi e i post sui wall.
Se non ci è possibile rimanere sempre collegati a questo social network, un’applicazione “ufficiale” come FbQuick può rivelarsi molto comoda. Si tratta di un software che cu notifica, direttamente sul desktop tutti i tipi di messaggi che coinvolgono Facebook, dalle “request” ai messaggi, passando per post nei “wall”, “pokes” e inviti. Lo possiamo scaricare direttamente dal sito ufficiale www.fbquick.com.

E per finire un tuffo nel passato. Non ci piacciono i cambiamenti apportati all’interfaccia nelle nuove versioni di Facebook? Possiamo toglierli, sfruttando lo script Undo New Facebook Redesign (http://userscripts.org/scripts/show/8482). È uno script che ci consente di applicare “l’undo” ai nuovi elementi dell’interfaccia.

Riccardo Meggiato

ANATOMIA DI UN MALWARE



Un'analisi dettagliata del funzionamento di un malware, nel contest Malware Challenge 2008

Lappiamo tutti, bene o male, che cosa è un malware e quali sono i suoi scopi; raramente però si ha modo di scoprire nel dettaglio come funziona un malware e come si compie la sua analisi. Ci viene incontro Anthony Lineberry, che partecipando al contest Malware Challenge 2008 ha documentato nei minimi particolari la sua analisi e ha preparato un PDF del risultato, recuperabile all'indirizzo http://blog.flexilis.com/wp-content/uploads/2008/12/malwarechallenge2008.pdf, mentre il blog dell'autore sull'argomento è all'indirizzo http://blog.flexilis.com/2008/12/the-2008-malware-challenge/.

:: Strumenti utili

Innanzitutto ricordiamoci che abbiamo a che fare con un malware, comunque sia è poco raccomandabile lasciarlo libero di fare scorribande sul nostro PC. Conviene preparare una macchina virtuale usando VMWare, in questo modo l'infezione sarà limitata al solo PC virtuale. Su questa macchina possiamo installare per esempio Windows XP SP2, abbastanza facile da gestire e abbastanza leggero. Gli strumenti effettivamente necessari sono diversi, alcuni commerciali altri freeware. Innanzitutto IDA Pro 5.0, celebre disassembler e debugger; seguono a ruota Windbg, Ollydbg con plugin Ollydump, PEiD, ImpRec, ProcessMon e Wireshark. Ecco come sono stati usati.

:: Comportamento del malware

Wireshark ha rilevato che il malware tentava di connettersi a un indirizzo Irc: molto probabile quindi che il cracker che l'ha creato lo controlli proprio via Irc e che il malware stesso contenga un bot. Anthony ha verificato che installando un server Irc locale e impostandone la voce corrispondente nel file hosts, in effetti il malware accede al server e si collega al canale #chalenge con password happy12. Analizzandolo con ProcessMon, sono state rilevate numerose variazioni alle chiavi di registro e la creazione di due file: a.bat, un file batch che si occupa di creare il secondo file, e 1.reg, che contiene le modifiche effettive al registro.
Queste modifiche sono per lo più dedicate al funzionamento delle connessioni TCP del computer infettato, ma sono interessanti due chiavi in particolare, che creano due voci in \\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run e in \\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices, che servono ad avviare automaticamente il malware all'avvio del Personal Computer.

:: Offuscamento

Per non essere rilevato dai programmi antivirus, l'eseguibile del malware è compresso e viene decompresso dinamicamente al momento dell'esecuzione. Per poter analizzare il programma è quindi necessario individuare con precisione il packer usato. PEiD rivela che si tratta di UPX, un packer molto diffuso: a questo punto usando Ollydbg con il plugin Ollydump, dopo aver impostato un breakpoint al termine della procedura di decompressione, è possibile salvare il disassemblato effettivo dell'eseguibile, per poterlo studiare con calma. ImpRec16 aiuta a ricostruire le tabelle delle procedure importate dalle DLL di sistema con nomi di più facile lettura, dato che il programma le carica in memoria e ne esegue le routine chiamandole per indirizzo e non per nome.

:: Analisi del disassemblato

La prima cosa che il malware compie una volta lanciato è implementare un proprio gestore di eccezioni, che si occupa prevalentemente di fare pulizia e chiudere le connessioni. Poi viene creato e lanciato il file a.bat, il quale, come già visto, è incaricato di creare e avviare a sua volta il file 1.reg. Dopo aver impostato le chiavi di registro per l'autoavviamento, si passa alla creazione della connessione su Irc.

Mentre la password è sempre la stessa, il nickname usato su Irc cambia secondo la posizione geografica, il sistema operativo usato e un numero casuale (per esempio USA[XP]803984): un'apposita routine si occupa di questo. Dopo aver effettuato il login il malware si trova nel loop principale: è in attesa di comandi dal cracker che, presumibilmente, si trova nello stesso canale Irc pronto a impartirli.

:: Il controllo del malware

Per poter controllare il malware bisogna collegarsi allo stesso canale Irc e impartire un comando di login con una password predefinita. La password è inserita direttamente nel codice del malware, ma non basta da sola a ottenere l'accesso: bisogna anche provenire da un dominio particolare, anch'esso codificato nel programma. Se si vuole provare a comandare il bot occorre quindi impostare il server Irc virtuale in modo che figuri come installato su quel dominio. Una volta ottenuto l'accesso, si ha un ampio ventaglio di possibilità. Attraverso la macchina infetta si può lanciare un server Web, un server FTP, attacchi di vario tipo (DDOS, ping flood, syn flood e altri) verso domini o altre macchine in rete, avviare una shell remota che dà accesso completo alla macchina vittima e molto altro ancora. Anthony non ha potuto, dati i tempi ristretti richiesti dal contest, analizzare in dettaglio tutti i comandi disponibili nel malware, ma già quelli elencati sono più che sufficienti per farsi un'idea.

(Codice 1)

La sezione che si occupa della connessione a Irc.

```
ABC0:00403B5B push 7Fh ; size_t
ABC0:00403B5D push offset aTestirc1_sh1xy ; "testirc1.sh1xy2bg.NET"
ABC0:00403B62 push offset byte_47554C ; char *
ABC0:00403B67 call _strncpy
ABC0:00403B6C mov eax, dword_41C7B8
ABC0:00403B71 push 3Fh ; size_t
ABC0:00403B73 push offset aChalenge ; "#chalenge"
ABC0:00403B78 push offset byte_4755CC ; char *
ABC0:00403B7D mov ds:dword_47569C, eax
ABC0:00403B82 call _strncpy
ABC0:00403B87 add esp, 40h
ABC0:00403B8A push 3Fh ; size_t
ABC0:00403B8C push offset aHappy12 ; "happy12"
ABC0:00403B91 push offset byte_47560C ; char *
ABC0:00403B96 call _strncpy
```


:: Conclusioni

Abbiamo qui riportato l'analisi condotta da Anthony, che comprende anche frammenti di codice reale. Per essere in grado di compiere un'analisi altrettanto accurata, e non solo per quanto riguarda il malware ma più ampiamente tutto il software che ci giunge in forma compilata, occorre una buona conoscenza del linguaggio Assembly dei moderni processori e avere discreta padronanza degli strumenti usati. In particolare, dobbiamo saper riconoscere lo strumento giusto per il compito che abbiamo davanti o l'obiettivo che vogliamo raggiungere. Questa è la base per studiare non solo malware e virus, ma anche sistemi di protezione, falle di sicurezza e, in definitiva, il funzionamento di tutto il software esistente. Come diceva Cypher, *"alla fine ti ci abitui: io neanche lo vedo più il codice, vedo solo belle biondine, brunette, e cosce lunghe"*...





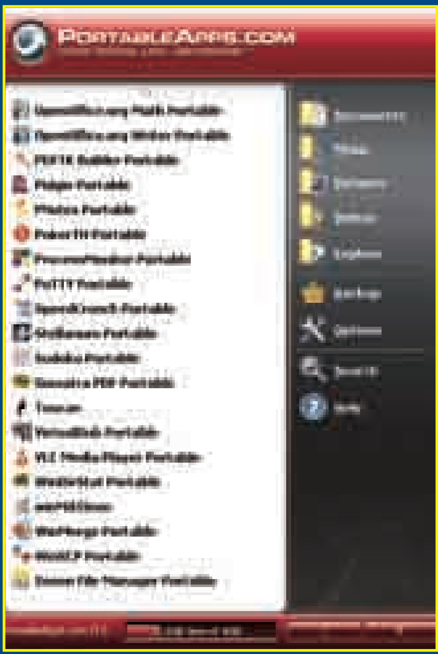
IL TUO COMPUTER IN TASCA

Con PortableApps.com rendiamo "portatili" i nostri programmi preferiti

Quando installiamo un'applicazione sul nostro computer, il software d'installazione compie diverse operazioni per preparare il sistema a eseguire il programma. Tra queste normalmente figurano la copia di nuovi file sul disco, la modifica del file di registro di Windows, l'installazione di elementi aggiuntivi eventualmente necessari per il funzionamento del programma e altro ancora. Spesso vengono aggiunte DLL nei posti più disparati, come la cartella di Windows o quella dei dati delle applicazioni (C:\Documents and Settings\NomeUtente\Dati Applicazioni, normalmente nascosta). Tutto questo rende estremamente difficile rendere l'applicazione installata "portatile" ovvero copiarla su una chiavetta USB per eseguirla su un altro computer. Ma è proprio così?

:: PortableApps.com

In effetti, molte applicazioni possono essere riconfigurate per poter essere eseguite direttamente senza "sporcare" il sistema che le ospita. È quello che fa PortableApps.com, un sistema che viene installato su una comune chiavetta USB che ci permette di portare con noi i nostri programmi preferiti. Non si tratta di versioni particolari: sono gli stessi software semplicemente impacchettati in maniera che possano essere eseguiti temporaneamente su un computer ospite senza che la configurazione di quest'ultimo venga modificata permanentemente. Esteticamente la suite PortableApps.com si presenta come un'icona nell'area di notifica, accanto all'orologio, che apre un menu simile al menu Start di Windows. Qui si trovano i vari programmi "portatili" utilizzabili. Tra questi troveremo esclusivamente programmi Open Source e liberamente distribuibili: benché in molti casi sia possibile, la distribuzione di applicazioni commerciali e Closed Source non è permessa per motivi legali. Abbiamo comunque un ampio ventaglio di possibilità: da OpenOffice.org a The Gimp, potremo giocare con Frets On Fire e



Il menu di avvio di PortableApps.com, del tutto simile al menu Start di Windows.

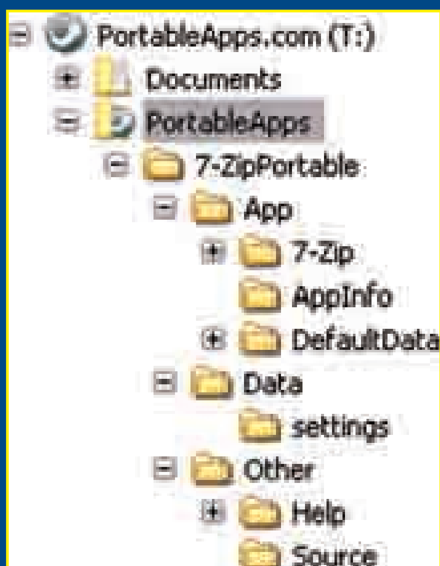
ascoltare musica con VLC, navigare sul Web con Firefox e scaricare la nostra posta con Thunderbird, mentre Sunbird organizza la nostra giornata.
In qualunque posto, su qualunque PC con Windows XP o Vista.

:: Ma come si fa?

Non è un'operazione molto semplice: occorre saper programmare, conoscere il funzionamento di Windows e delle sue applicazioni e disporre di tempo e pazienza per studiare la (poca) documentazione disponibile.
La tecnologia di PortableApps.com si basa su NSIS, il software di installazione gratuito di Nullsoft che è liberamente scaricabile dal sito www.nullsoft.com. Con questo software si creano pacchetti di installazione che contengono l'applicazione e tutti i file di configurazione necessari per renderla portatile e poterla eseguire dalla chiavetta USB.
In effetti, dato che il requisito di un'applicazione portatile è quello di non lasciare assolutamente nulla sul PC ospite dopo la sua esecuzione, dovranno essere preparati script di installazione che aggiungono al file di registro le chiavi necessarie al programma, copiano i file e le DLL nelle cartelle adeguate, avviano l'applicazione e, alla sua chiusura, rimuovono tutti i file e le modifiche temporanee apportate al sistema. Di questo si occupa un particolare file eseguibile, che viene chiamato launcher.

:: Struttura delle cartelle

Il sistema di PortableApps.com risiede su una chiavetta USB, meglio se dedicata esclusivamente a questo scopo e di capienza adeguata (4 GB vanno benissimo). Nella cartella principale si trovano il file eseguibile StartPortableApps.exe che serve per avviare il menu principale, il file Autorun.inf che rende autoavviabile la chiavetta, la cartella PortableApps che funziona come la cartella Programmi di Windows e la cartella Documents, per salvare i nostri documenti.



La tipica struttura di cartelle di una chiavetta USB trasformata in una chiavetta PortableApps.com.

In PortableApps, tutte le applicazioni hanno una cartella dedicata, chiamata con il nome dell'applicazione stessa seguito da "Portable" (per esempio "FirefoxPortable"). In questa cartella si trovano diverse sottocartelle, secondo uno schema prestabilito, e due soli file: il launcher e il file HTML della guida in linea. In App troviamo le sottocartelle AppInfo (per informazioni generiche sull'applicazione), DefaultData (in cui trovano posto eventuali file di supporto dell'applicazione) e una cartella con l'applicazione, di solito chiamata come



Lo splash-screen personalizzato del launcher per le applicazioni portatili.

la medesima e contenente l'eseguibile e tutti i file necessari per la sua esecuzione. In Data trovano posto file di configurazioni particolari del programma, se necessari. In Other si trovano la cartella Help, che normalmente contiene le immagini per la guida HTML dell'applicazione portatile, e la cartella Source, in cui è possibile distribuire i sorgenti dell'installer NSIS della stessa.

:: La procedura

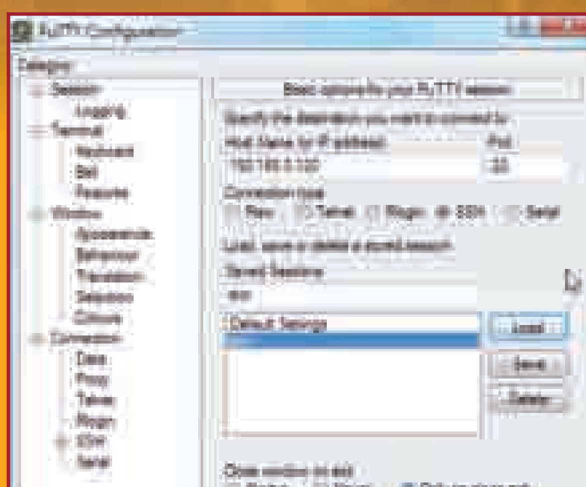
Innanzitutto è meglio partire da un'installazione pulita di Windows. A questo scopo è utile una macchina virtuale creata con VMWare, VirtualBox o VirtualPC, programmi che si possono ottenere gratuitamente. Questo perché in questo modo si ha a disposizione un ambiente ottimale, senza programmi in esecuzione in background come antivirus e simili. Occorre poi un software che sia in grado di compiere scansioni del sistema e del file di registro per vedere che modifiche vengono fatte a Windows dall'applicazione che si vuole rendere portatile. RegShot, un programma gratuito, è adattissimo a questo scopo: lo avviamo, compiamo la prima scansione del sistema pulito, installiamo il nostro programma e lo avviamo un paio di volte, poi compiamo una seconda scansione e chiediamo a RegShot di confrontare i due risultati. Avremo quindi una panoramica delle chiavi di registro e dei file usati dall'installazione del programma e dal programma stesso.
Questi dati servono per modificare i file sorgenti dell'installer NSIS e del launcher che vanno creati per rendere l'applicazione portatile, partendo dai template disponibili su PortableApps.com nell'area Development, dove si trovano tutte le informazioni utili per applicare lo stesso sistema ad altri programmi.

Trasformiamo uno storage di rete in una perfetta macchina per scaricare i torrent



Hacking & Download

La distribuzione di file tramite il sistema Torrent permette di ottimizzare gli scambi di file tra le diverse fonti. Purtroppo, molti file torrent restano comunque piuttosto lunghi da scaricare e ci costringono a tenere acceso il computer per lunghi periodi. Se, poi, il computer è portatile, il download di uno o più file torrent ci impedisce di disconnetterlo e, quindi, di portarcelo in giro, pena la perdita di tempo nel recupero dei download. A pensarci bene, inoltre, la potenza dei nostri computer è totalmente sprecata per i download: non serve un processore veloce ma ne basta uno mediocre, con una connessione di rete qualsiasi e molto spazio su disco, per poter scaricare quello che vogliamo. A rispondere esattamente a queste caratteristiche sono alcuni dischi esterni come alcuni MyBook prodotti dalla Western Digital. I WD MyBook World Edition I e II, così come il WD ShareSpace, sono composti da uno o più dischi a cui è accoppiata una scheda madre in cui è installata una versione embedded di Linux e dispongono di una scheda di rete, usata per collegarli alla rete casalinga o aziendale. Sulla carta c'è tutto il necessario per trasformare una di queste unità di storage in un sistema di download autonomo e perfetto, liberando



Putty è gratuito, si scarica dal sito www.chiark.greenend.org.uk/~sgtatham/putty ed è lo strumento principe per l'accesso ai dispositivi con software embedded.

il nostro computer da questa incombenza. Naturalmente, la modifica di questi dispositivi invalida la garanzia del produttore ma, viste le loro potenzialità, in molti casi vale la pena rischiare.

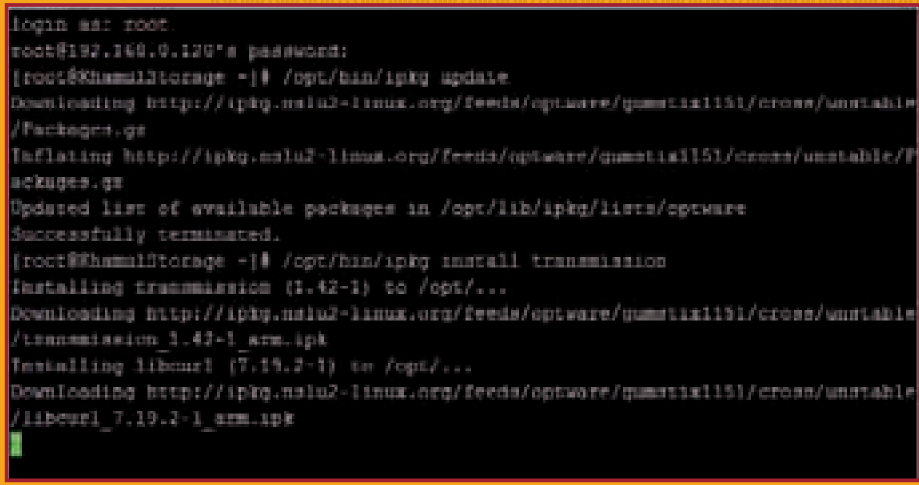
:: Via i lucchetti

La prima cosa da fare è quella di trovare il sistema di accedere direttamente al sistema operativo del disco, bypassando l'interfaccia Web di gestione standard. Per farlo occorre usare un trucco: per aggiornare il suo firmware, questo tipo di dischi effettua un collegamento Web a un sito prestabilito e basta confondere un po' le carte per far eseguire al dispositivo uno script diverso. Entriamo nell'interfaccia Web di gestione del disco inserendo il nostro nome e la nostra password. Poi accediamo all'aggiornamento del firmware dell'unità e modifichiamo la parte finale dell'indirizzo con la scritta **?fwserver=mybook1.110mb.com/firmware.php.** Dovremo ottenere una scritta simile a quella in **Figura 1**:

[Figura 1]

```
http://192.168.10.120/auth/firmware_upgrade.pl?fwserver=mybook1.110mb.com/firmware.php
```

Premiamo Invio e poi clicchiamo su Download and Install per aggiornare il firmware. Nella realtà, il disco starà solo sbloccando un protocollo di accesso chiamato SSH, tramite cui accederemo alle sue funzioni di base. Dopo qualche minuto, il gioco sarà fatto e il dispositivo sbloccato. Ora abbiamo bisogno un programma di gestione del protocollo SSH per accedere al disco.
Tra i migliori e gratuiti in circolazione c'è Putty. Scarichiamolo dal sito http://www.chiark.greenend.org.uk/~sgtatham/putty/ e installiamolo. Una volta avviato, inseriamo l'indirizzo del nostro disco di rete, lasciando le altre impostazioni inalterate, e ci troveremo davanti alla consolle di Linux. Inseriamo ora il nome di accesso che usiamo anche per l'interfaccia Web standard e la password corrispondente per aprire una sessione autenticata.



Una volta ottenuto l'accesso al disco tramite Putty, l'installazione delle utility procede come per qualsiasi versione standard di Linux.

Ora basterà dare il comando **su-**, senza password, per diventare amministratori di root del sistema. Impostando una password, come per qualsiasi altra versione di Linux, potremo accedere al sistema direttamente con l'account di root.

:: Qualche utility

Il passo successivo sarà quello di installare qualche pacchetto di software utile alla nostra sopravvivenza. Purtroppo, la versione di Linux a nostra disposizione è veramente ridotta all'osso. Per prima cosa installiamo il gestore di pacchetti OptWare, con cui installeremo tutto il resto. Per farlo basta recuperarlo come se fossimo in una normale installazione Linux, tramite i feed.

Basta usare la sequenza di comandi indicati nella **Figura 2**, in basso.
A questo punto OptWare è installato ma a causa delle caratteristiche del Linux a nostra disposizione dovremo aggiungere un parametro al file di configurazione di ld. Basterà dare due ultimi comandi:

```
echo "/opt/lib" >>/etc/ld.so.conf
ldconfig
```

Dopo questa installazione potremo, finalmente, installarci un buon editor di testi, come Nano, adattissimo al nostro disco esterno.
Basta farlo usando OptWare:

```
/opt/bin/ipkg install nano
```

Con Nano potremo aprire **/etc/inittab** e aggiungere la riga seguente, per rendere l'SSH disponibile anche in caso di riavvio del disco:

```
sysinit:/usr/sbin/sshd
```

A questo punto, il sistema Linux presente sul disco esterno è pronto per essere plasmato a nostro piacimento e potremo usarlo come una normale distribuzione Linux.

[Figura 2]

```
feed=http://ipkg.nslu2-linux.org/feeds/optware/gumstix1151/cross/unstable
ipk_name=$(wget -qO- $feed/Packages | awk '/^Filename: ipkg-opt/ {print $2}')
wget $feed/$ipk_name
tar -xOvzf $ipk_name ./data.tar.gz | tar -C / -xzvf -
sed -i -e 's|/stable|/unstable|' /opt/etc/ipkg.conf
```

:: Via ai download

Per creare un sistema di download di file torrent dobbiamo installare Transmission, un client molto famoso in ambiente Linux ma disponibile per diverse piattaforme. Sempre ricorrendo a OptWare, basterà dare i comandi descritti in **Figura 3**:

[Figura 3]

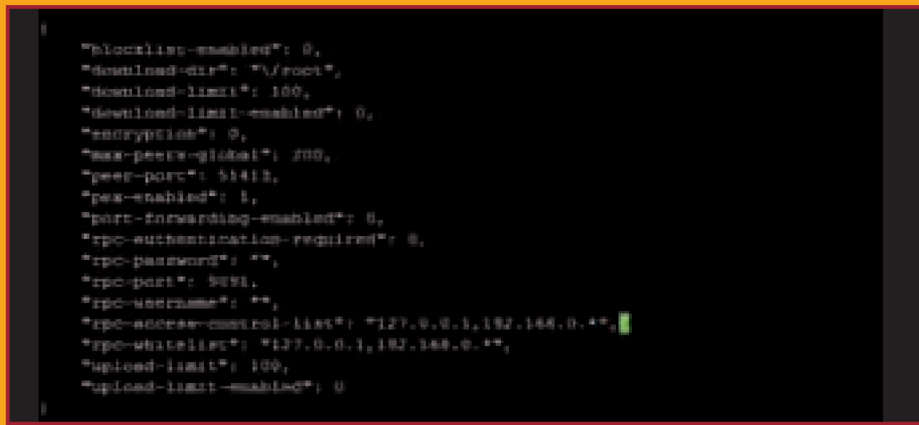
```
/opt/bin/ipkg update
/opt/bin/ipkg install transmission
ldconfig
/opt/bin/ipkg install libiconv
ldconfig
```

Una volta completata l'installazione, possiamo avviare Transmission usando il comando seguente:
/opt/bin/transmission-daemon

Nella maggior parte dei casi, però, questo non basterà a permetterci l'accesso libero al sito di download: come impostazione standard, Transmission accetta le connessioni solo se provengono dalla machina stessa, dall'IP 127.0.0.1. Sarebbe scomodo utilizzare il sistema SSH per indicare i nostri download quando Transmission ci mette a disposizione una comoda interfaccia Web.

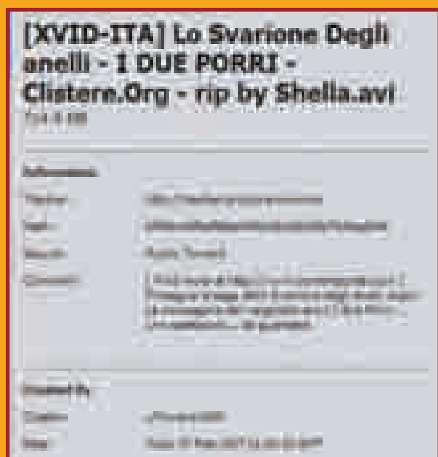


Il sito Web che attiviamo sulla porta 9091 permette in modo banale il controllo dei download e l'impostazione delle nostre preferenze di funzionamento.



Usiamo nano, editor di testi di base, per modificare le impostazioni di default di Transmission e permettere l'accesso al sistema da qualsiasi Ip della nostra rete LAN.

Per fare qualsiasi modifica dovremo fermare il processo di Transmission con il comando seguente:
killall transmission-daemon



Come i migliori client, Transmission ci permette di consultare varie informazioni sui file in download: dimensioni, tempo previsto di completamento, hash del file e via dicendo.

Poi, ricorrendo a un editor di testi, dovremo modificare il file **/root/.config/transmission-daemon/settings.json** modificando le righe seguenti. Ovviamente, se abbiamo una rete di classe diversa a quella 192.168.1, dovremo adattare i dati inseriti al nostro caso personale, vedi **Figura 4**.

[Figura 4]

```
"rpc-access-control-list": "127.0.0.*,192.168.1.*",
"rpc-whitelist": "127.0.0.1,192.168.1.*",
```

Salviamo il file, riavviamo Transmission e colleghiamoci con il nostro browser all'indirizzo corrispondente al nostro disco, sulla porta 9091:
http://192.168.10.120:9091/

Ci troveremo un'interfaccia Web pronta per accogliere le nostre richieste di download.



L'installazione di programmi aggiuntivi invalida la garanzia ma mantiene perfettamente funzionante l'interfaccia standard di gestione del disco.


CREA IL TUO SITO DI
HACKER JOURNAL
Realizza il sito di Hacker Journal così come lo vorresti, pubblicalo in un area non indicizzata del tuo spazio Web e inviaci il link.
I migliori cinque, a insindacabile giudizio della redazione, verranno presentati nella home page di hackerjournal.it dove i lettori potranno votare ed eleggere il primo classificato.
Il sito vincitore verrà utilizzato, interamente, o esculsivamente come template grafica, come sito ufficiale di Hacker Journal.
Invia una mail all'indirizzo sito@hackerjournal.it con il link per visualizzarlo, i tuoi dati e una dichiarazione liberatoria di utilizzo.
www.hackerjournal.it

PICODRIVE





Il caro vecchio SEGA megadrive rinasce a bordo del nostro telefonino

Chi non ha mai giocato con una console (o non continua a farlo) alzi la mano! Un tempo era guerra tra PC e Amiga e quando il PC stava ormai vincendo, spinto da legioni di cloni, dalle prime schede audio e da vere schede video, vennero lanciate sul mercato console dedicate esclusivamente al gioco, che garantivano prestazioni decisamente superiori a quelle cui eravamo abituati, anche se lontane anni luce da, per fare un esempio, una Playstation 3. Tra queste ebbe molto successo il SEGA Megadrive che molti ricorderanno anche grazie alla sua mascotte, Sonic The Hedgehog. Con le console arrivarono anche molti giochi che riempirono le ore di adolescenti e universitari e qualche appassionato, o nostalgico dei bei giorni di gioventù, continua ad amare se non addirittura a preferire, i vecchi titoli nonostante gli effetti speciali delle console dei giorni nostri. Per andare incontro a questi desideri e per amore delle sfide, sono nati diversi emulatori che hanno permesso di giocare ancora con questi vecchi titoli anche su piattaforme diverse dalle originali, come i PC e di recente anche altre console. Oggi è possibile trasformare anche il proprio telefonino con symbian in un emulatore all'altezza del compito, grazie alla notevole potenza di calcolo dei processori. E PicoDrive è proprio il porting dell'emulatore di SEGA Megadrive per Symbian.

:: L'emulatore e le ROM

Il software è gratuito, diffidate quindi dei siti che propongono il download a pagamento o a seguito di iscrizione. Due link dove trovare l'emulatore per diverse versioni di symbian sono:

per S60 2nd version:
http://phonesymbian.com/wpcontent/uploads/2007/12/picodrives602nd060.zip

per S60 3rd version:
http://phonesymbian.com/wpcontent/uploads/2007/01/picodrive0_50_3rd.zip

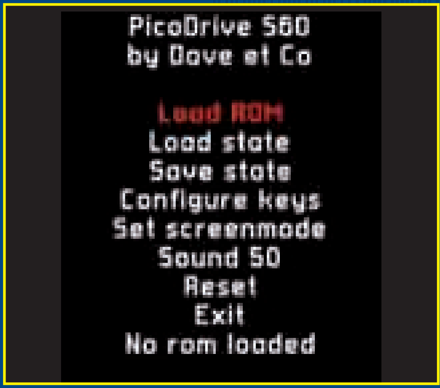
L'installazione è davvero semplice: basta scompattare l'archivio e installare il sis tramite PC Nokia Suite. Il software "emula" l'hardware delle console, permettendo di scegliere persino il tipo di chip audio che si preferisce, ma non ha alcun gioco a bordo, ossia nessuna ROM. Sulle ROM la questione è controversa, dal momento che si parla di codice proprietario ancora protetto da copyright che tra l'altro non è più nemmeno in commercio (escludendo le vendite di ebay). Ricordiamo quindi che, dal punto di vista legale, la ROM andrebbe utilizzata solo

da parte del legittimo proprietario di una versione originale del gioco (e magari con l'autorizzazione comunque del produttore); di fatto esistono numerosi siti che permettono il download (e la conservazione di tanti giochi introvabili) che il fenomeno viene in pratica tollerato, almeno per quanto riguarda le ROM di console non più in commercio (dove quindi l'utilizzo di ROM non compromette un business oramai decaduto). Un sito tra i tanti è **www.romnation.net** e viene consigliato di scaricare le ROM in cui compare un punto esclamativo a indicare un corretto e fedele dumping della memoria originale.



:: Installazione e uso

Si può scegliere liberamente se installare l'emulatore nella memoria del telefono o nella memoria esterna, lo stesso dicasi per le ROM che suggerisco chiaramente di installare in quella d'espansione. Non è necessario alcun accorgimento in particolare, si può quindi creare una cartella ROM in cui copiare tutte quelle con cui si potrà giocare. Il programma viene installato nel menu principale e una volta lanciato presenta un menu molto semplice e intuitivo.



Il menu di Picodrive.

:: PicoDrive in azione

L'emulatore supporta i cheats (Game Genie) e patch ROM; è stato implemento il soft-reset che riavvia la ROM senza doverla ricaricare. Si può scegliere il formato dello schermo preferito (portrait, full resolution, anche con lo scroll orizzontale durante il gioco) e il tipo di render (da cambiare solo se si riscontrano dei problemi grafici). È possibile attivare un controllo più accurato sulla sincronia del gioco e sugli sprite, che chiaramente impattano con la velocità e la fluidità di gioco. È possibile che la ROM possa essere bloccata su una macroregione (come i DVD), ma è presente un selettore che permette di scegliere quella corretta. La voce **Load ROM** attiva il browser per caricare la ROM, **Load/Save** permettono di congelare il gioco in formato compresso. Durante il gioco, se sembra che si stia perdendo la sincronia con l'audio basta



Il file browser per la scelta della ROM.



premere la "C" due volte per sistemare il problema. Una sola volta durante il gioco ci riporta al menu dell'emulatore. Se durante il gioco arriva una telefonata, un avviso di "Batteria scarica" o si passa a un'altra applicazione è possibile che il telefono si blocchi completamente. Quindi prima di compiere una di queste operazioni conviene andare al menu principale. Nel caso la velocità di gioco sia troppo lenta o addirittura l'emulatore vada in crash, conviene abilitare tutti e tre i chip audio, "accurate sprites" e "accurate timing" e disabilitare "alt. render". Nel caso ci siano ancora problemi, abilitare "alt. render" e se non funziona neanche in questo caso è bene fare un report su questo gioco per comunicare che non funziona! Non tutti i giochi infatti sono del tutto compatibili (ad esempio "Virtua Racing" non funziona perché manca l'emulazione del Sega Virtua Processor).

Massimiliano Brasile



Il menu di configurazione video.

Una nuova frontiera delle tecnologie Open per gli appassionati di elettronica

HARDWARE LIBERO

Open Source è un'espressione entrata ormai nell'uso comune di tutti gli appassionati di informatica e sappiamo bene che cosa significa: software di libero utilizzo che rende disponibile anche il proprio codice sorgente. Generalmente quando si parla di Open Source si pensa subito a un software, ad archivi contenenti file sorgente in vari linguaggi di programmazione e alla possibilità di adattamento e di espansione che questo sistema di distribuzione dei programmi offre.

:: La nuova scommessa

Questo concetto è stato recentemente allargato anche all'hardware, anche se di primo acchito non si riesce bene a capire che cosa abbiano in comune l'hardware libero e il software libero. L'Open Source Hardware, spesso chiamato più brevemente Open Hardware, è in realtà molto simile all'Open Source inteso più generalmente come software. Avere a disposizione un oggetto Open Hardware significa anche disporre dei suoi schemi elettrici, della componentistica, dei disegni in formato elettronico della PCB e di tutte le informazioni tecniche che stanno dietro il suo funzionamento e che possono tornare utili per modificarlo, migliorarlo o anche semplicemente ripararlo da soli. Il vantaggio di questo sistema è presto detto: mentre in un sistema Closed non possiamo fare altro che usare passivamente quanto il produttore ha specificamente previsto per il proprio prodotto (fatto salvo un bel lavoro di reverse engineering dell'hardware, che però non sempre è alla portata di tutti), usando un sistema Open possiamo capirne il funzionamento più intimo e, se abbiamo le adeguate conoscenze tecniche, adattarlo facilmente ai nostri scopi armandoci di saldatore.



Un progetto Open Hardware: Aurora 224, un mixer per DJ a due canali con 24 potenziometri analogici, 3 slider e diversi LED di segnalazione.

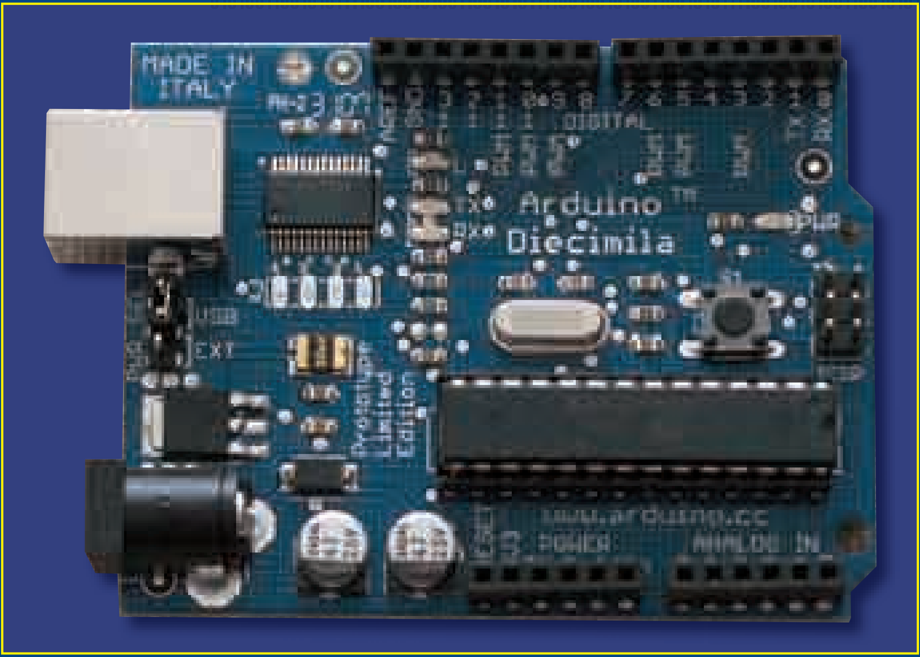
:: Open non significa gratis

Che nel mondo del software Open Source spesso significhi anche software gratuito non è una verità assoluta: i termini "Open" e "gratis" significano cose differenti e possono non essere uno conseguenza dell'altro. Un programmatore può continuare a vendere il proprio programma, pur rendendone disponibili i sorgenti ma vietandone la distribuzione, rendendo di fatto il possesso del codice sorgente un vantaggio solamente per chi lo ha regolarmente acquistato.

Lo stesso vale, a maggior ragione, nel campo dell'Open Hardware, dove i componenti elettronici hanno un costo che prescinde dalla volontà di chi progetta un dispositivo aperto. Non troveremo quindi apparecchiature Open Hardware gratuite, anche se di solito i costi sono contenuti, ma dopo averle comprate potremo modificarle liberamente secondo le nostre esigenze. Addirittura, potremmo trovare schemi e documentazione di un dispositivo gratuitamente, ma occorrerà comunque comprare i componenti necessari in un negozio di elettronica oppure online per poterlo costruire.

:: Disponibilità

Parliamoci chiaro, non troveremo in circolazione un lettore DVD Open Hardware, nemmeno un televisore o un forno a microonde. Molto più facilmente ciò che potremo trovare nel mondo dell'Open Hardware sono (relativamente) semplici circuiti modulari, quasi tutti legati al mondo dei microcontroller e spesso legati al mondo dell'informatica, per esempio circuiti che, collegati alla porta parallela o ad altra uscita del PC permettono di controllare dispositivi esterni. Detto così non pare che abbiano tutto questo appeal, dopotutto è abbastanza noioso montare una manciata di componenti su una basetta per pilotare dei LED con la porta parallela del PC. In realtà è qui che interviene il vantaggio dell'Open Hardware: lo schema di base lo possiamo modificare come vogliamo e quindi adattarlo alle nostre esigenze. Che ne dite di controllare gli impianti anti-intrusione di casa dal PC con una schedina micro controller opportunamente programmata, o creare un display esterno LCD che ci mostri costantemente lo stato del nostro personaggio durante interminabili battaglie in un gioco di guerra online, o ancora pilotare i nostri strumenti musicali MIDI direttamente dal computer ma senza comprare un dispendioso dispositivo dedicato?



Arduino Diecimila, versatile prodotto Open Hardware di tecnologia italiana e apprezzato in tutto il mondo.

:: Il re dell'Open Hardware

Un prodotto Open Hardware che sta prendendo molto piede tra gli appassionati di elettronica e informatica congiunte in tutto il mondo è Arduino. Si tratta di una piattaforma di progettazione elettronica aperta e flessibile, progettata e costruita in Italia, basata su microcontroller e particolarmente adatta per costruire piccoli computer programmabili: oltre al microprocessore (un microcontroller Atmel) e alla sua circuiteria di base, offre sulla stessa basetta uno spazio per prototipi che può essere usato per collegamenti con il PC o con altre basette, piccoli circuiti e dispositivi di visualizzazione. È disponibile in diverse versioni, di dimensioni e capacità differenti, tutte comunque adattabili ai propri progetti e tutte rigorosamente Open. Comprando uno di questi kit avremo a disposizione tutti gli schemi, la documentazione e le specifiche, e possiamo scaricare liberamente il kit di sviluppo software che è costituito da un IDE basato su piattaforma Java, quindi eseguibile su qualunque sistema operativo.

:: Licenze Open Hardware

Sostanzialmente, i prodotti Open Hardware adattano alla nuova ambientazione le licenze Open già esistenti nel campo del software. Si tratta di un approccio più comodo rispetto alla creazione ad hoc di nuove licenze, che non farebbe altro che apportare ulteriore confusione oltre a quella già presente a causa della molteplicità e delle sottili differenze tra le licenze software disponibili. Sono state avanzate comunque delle proposte per aggiornare queste ultime alla nuova realtà. La differenza di base è l'applicazione sul copyright (come concetto di opera di ingegno) nel caso del software, mentre nel caso dell'hardware ciò che le licenze proteggono è il patenting, ovvero il brevetto delle tecnologie.

Privateer

L'attacco di Denial of Service basato sugli sms, che fa impazzire il colosso finlandese.

Curse of silence: la maledizione dei Nokia

Se vi dicessero che il vostro telefonino con Symbian a bordo può essere reso totalmente insensibile agli sms senza che voi ve ne accorgiate, ci credereste? Ebbene è possibile: Tobias Engel ha pubblicato una specifica dettagliata riguardante una falla di Symbian. L'attacco si configura come un Denial of Service da remoto, trasmesso per mezzo di sms/mms ed è stato soprannominato "Curse of Silence" per l'effetto che provoca: il telefono vittima non notifica l'arrivo del messaggio malizioso, ma successivamente non sarà più in grado di ricevere ulteriori messaggi finché non verrà effettuato un hard-reset (che riporta il telefono alla condizione di fabbrica con perdita di tutti i dati di rubrica, applicazioni, download effettuati, link del browser...).

Le versioni di Symbian con la falla sono tutte quelle rilasciate sui Nokia serie 2.6, 2.8, 3.0 e 3.1, il che equivale a dire che praticamente quasi ogni Nokia con Symbian ne è affetto.
Il rischio viene giudicato di criticità media per le versioni S60 2.8 e 3.1, perché durante l'attacco il dispositivo non sarà in grado di ricevere altri sms o mms e successivamente potrà riceverne solo alcuni fino al reset hardware; viene giudicato ad alta criticità invece per le versioni 2.6 e 3.0, perché a seguito dell'attacco non potrà ricevere più sms o mms fino al reset!



:: La falla

Lo standard 3GPP TS 23.040 specifica quale debba essere il metodo per inviare e-mail via sms. In particolare, viene specificato che per questo formato, l'sms inizi o con il campo **from-** o **to-email-address** seguito dallo spazio e poi dal messaggio. In questo caso l'identificativo del messaggio sms deve essere impostato come "Internet Electronic Mail". Lo standard non specifica però come debba apparire tale messaggio in ricezione sul telefono del destinatario, scelta che è lasciata al costruttore (Nokia in questo caso).

Prima della versione 2.6 di S60 i messaggi venivano visualizzati esattamente come erano spediti, mentre a partire dalla versione 2.6 quando la parte del messaggio che dovrebbe contenere l'indirizzo del mittente sembra un indirizzo e-mail (ad esempio compare la @ da qualche parte), tale campo viene visualizzato come e-mail mittente invece che come TP-Originating-Address.

Se questo campo è più lungo di 32 caratteri, le quattro versioni incriminate di Symbian falliscono nella visualizzazione del messaggio o nella notifica del loro arrivo sull'interfaccia, ma inviano al centro messaggi la conferma di averlo ricevuto. Se viene quindi inviata una e-mail tramite sms avente la seguente formattazione:

<indirizzo e-mail>
+ SPAZIO
+ <corpo del messaggio>

dove l'indirizzo e-mail contiene più di 32 caratteri, tutti i dispositivi con a bordo la serie 60 (2.6, 2.8, 3.0, 3.1) non potranno ricevere ulteriori sms o mms: in particolare, le versioni 2.6 e 3.0 si bloccheranno subito dopo il primo sms, mentre la 2.8 e la 3.1 dopo 11 di questi messaggi.
Nelle versioni 2.8 e 3.1, dopo aver ricevuto l'undicesimo sms malformattato, su ricezione di un ulteriore sms (anche sano) viene visualizzato un messaggio di warning che avvisa l'utente di aver finito lo spazio di memoria, anche se la cartella che contiene i messaggi in arrivo è vuota, cosa che per lo meno dovrebbe insospettire l'utente.

A questo punto, un riavvio del telefonino non risolve la situazione, perché sarà sì in grado di ricevere gli sms di nuovo, ma questi verranno spezzati in più parti e verrà ricevuta solo la prima parte. Inoltre il telefono visualizzerà comunque il warning per mancanza di memoria. Riavviando nuovamente il telefono, verrà ricevuta la seconda parte del messaggio e, se ne esiste una terza parte, al successivo riavvio arriverà anche quella e così via.

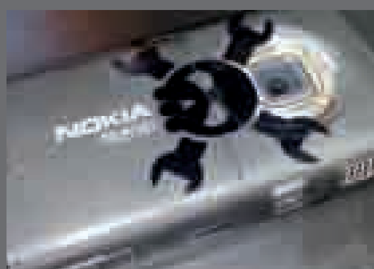
I NOKIA A RISCHIO

Se non si è sicuri di avere una deterS60 3rd Edition, Feature Pack 1 (S60 3.1): E90 Communicator, E71, E66, E51, N95 8GB, N95, N82, N81 8GB, N81, N76, 6290, 6124 classic, 6121 classic, 6120 classic, 6110 Navigator, 5700 XpressMusic

S60 3rd Edition, initial release (S60 3.0): E70, E65, E62, E61i, E61, E60, E50, N93i, N93, N92, N91 8GB, N91, N80, N77, N73, N71, 5500, 3250

S60 2nd Edition, Feature Pack 3 (S60 2.8): N90, N72, N70

S60 2nd Edition, Feature Pack 2 (S60 2.6): 6682, 6681, 6680, 6630



:: Come viene realizzato l'attacco

Per generare l'attacco, non è necessario un hardware particolare: è sufficiente avere un telefonino o un modem che supporti i comandi AT secondo lo standard 3GPP TS 27.005, ad esempio usare proprio uno dei Nokia affetti dal problema o uno storico 6310i, che ha addirittura un'opzione dedicata nel menu che configura automaticamente la spedizione del messaggio come e-mail.
È sufficiente quindi conoscere il numero associato alla sim inserita nel telefonino "bacato" e inviare il messaggio d'attacco.

:: Come difendersi

Non è possibile dal lato utente risolvere il problema perché si tratta di un baco firmware. Finché Nokia non rilascerà una nuova versione per ogni modello affetto quindi la falla resterà aperta e visto il numero di terminali in gioco non sarà certo chiuso in breve tempo. Di conseguenza, si è saputo che Nokia sta lavorando con gli operatori mobili per richiedere un blocco selettivo di questo tipo di messaggi sui loro network. Alcuni hanno accettato (come H3G Austria), ma non tutti. Il filtro viene applicato sui messaggi che presentano il TP-PID "Internet Electronic Mail" e un indirizzo e-mail che ha più di 32 caratteri. Il blocco agisce anche sugli mms, dal momento che la segnalazione del loro arrivo arriva tramite sms.

Per ripristinare il corretto funzionamento del telefono l'unica soluzione sembrava essere l'hard-reset (che si ottiene inserendo il codice *#7370# da modalità base), ma fortunatamente è ora disponibile un tool gratuito distribuito da Fortinet (www.fortiguardcenter.com/mobile/cleanup.html) che permette di rimuovere gli sms malevoli già ricevuti (che non possiamo vedere) e bloccarne l'arrivo di nuovi se l'applicazione è in esecuzione. Consigliamo quindi di installare quanto prima il tool, e fare una scansione completa del telefono.